中華電信 HiPKI 憑證管理中心（OVTLSCA）

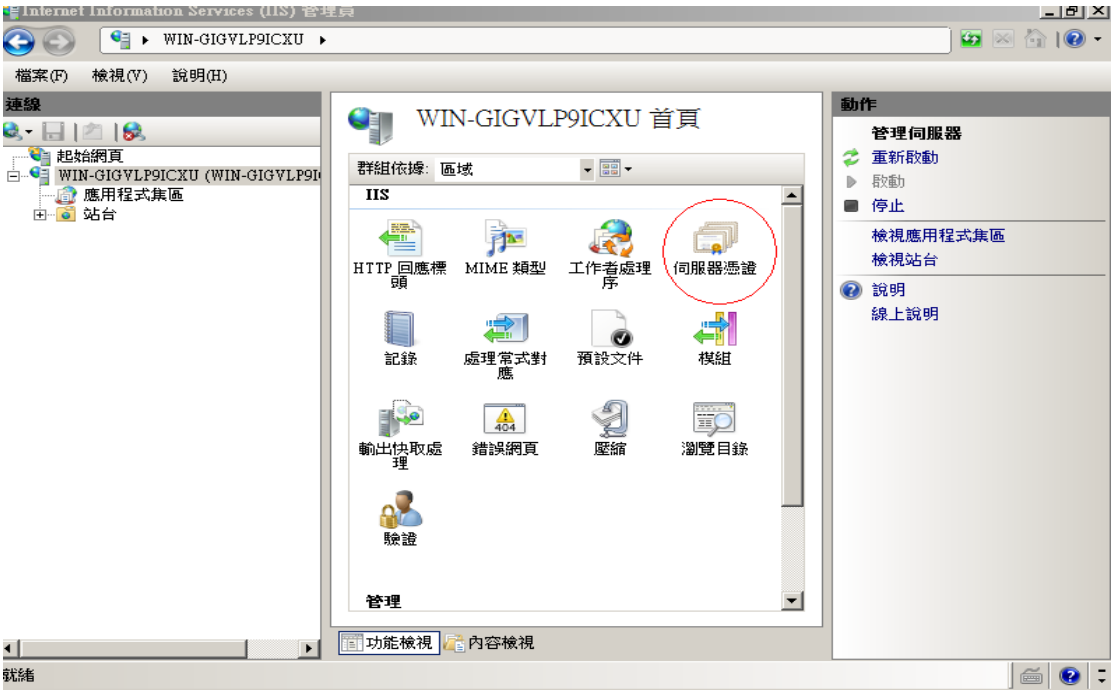
Windows IIS 7.0 SSL 憑證請求檔製作與憑證安裝手冊

聲明：本手冊之智慧財產權為中華電信股份有限公司（以下簡稱本公司）所有，本公司保留所有權利。本手冊所敘述的程序係將本公司安裝相關軟體的經驗分享供申請 SSL 伺服軟體憑證用戶參考，若因參考本說明文件所敘述的程序而引起的任何損害，本公司不負任何損害賠償責任。

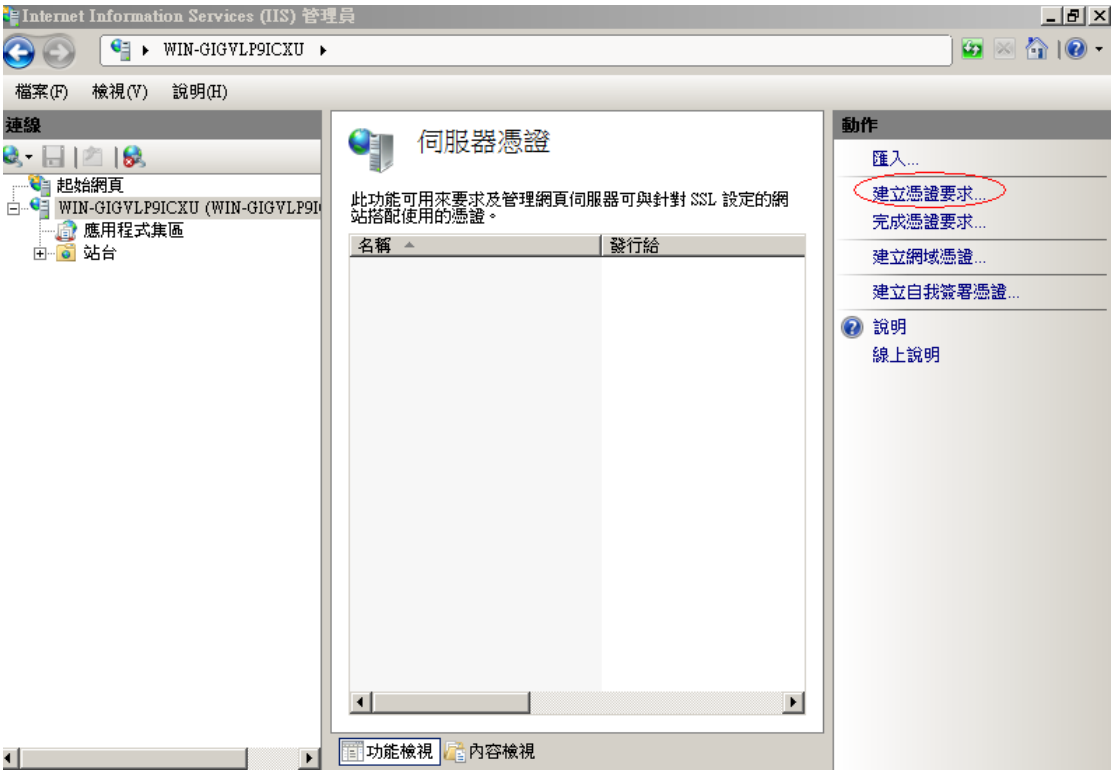
目錄

Windows IIS 7.0 SSL 憑證請求檔製作手冊

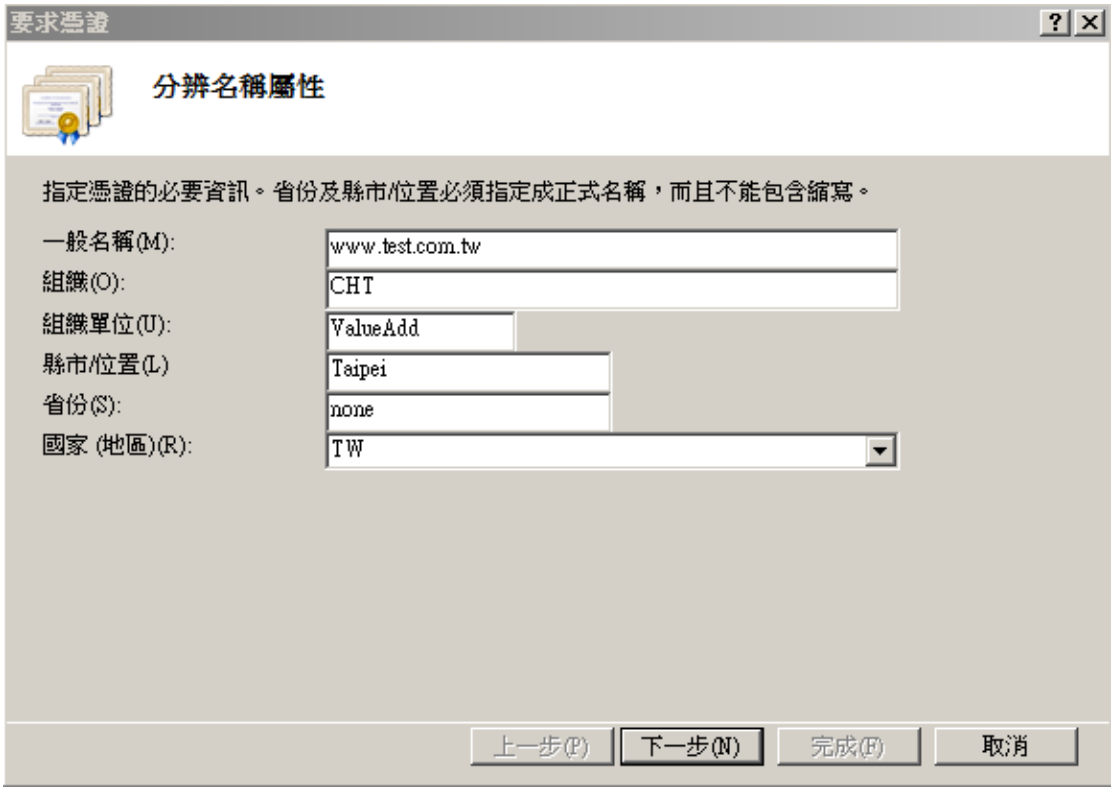
一、開啟「Internet Information Services (IIS)管理員」並點選主機連線預設名稱(預備申請與安裝 SSL 憑證的網站)，再點選畫面右邊「伺服器憑證」兩下。



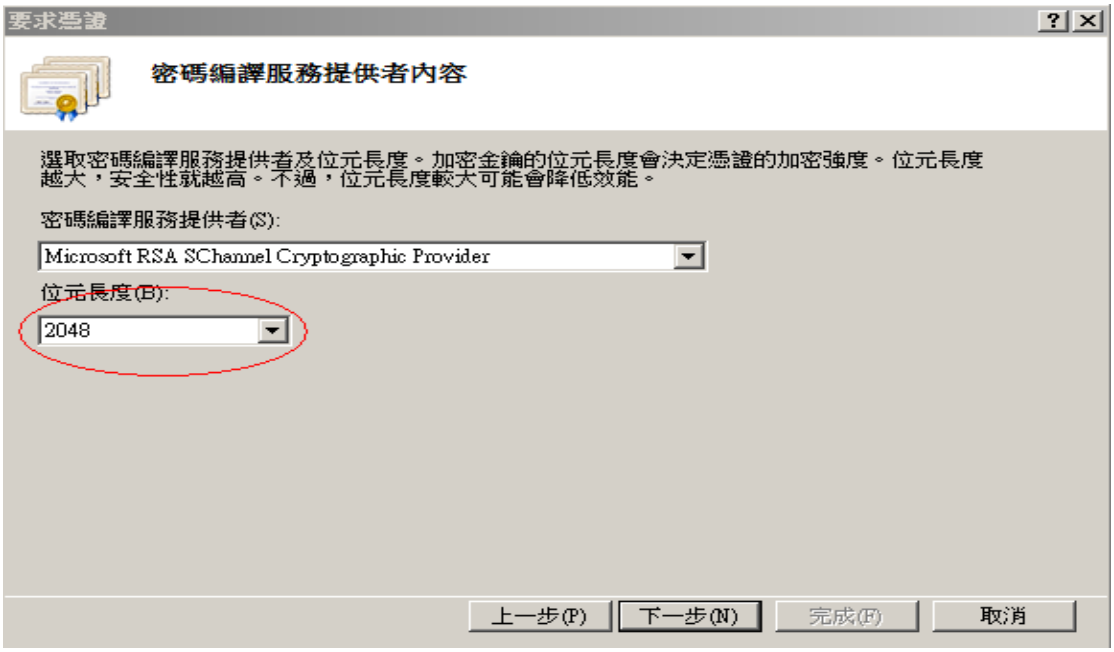
二、點選「建立憑證要求」



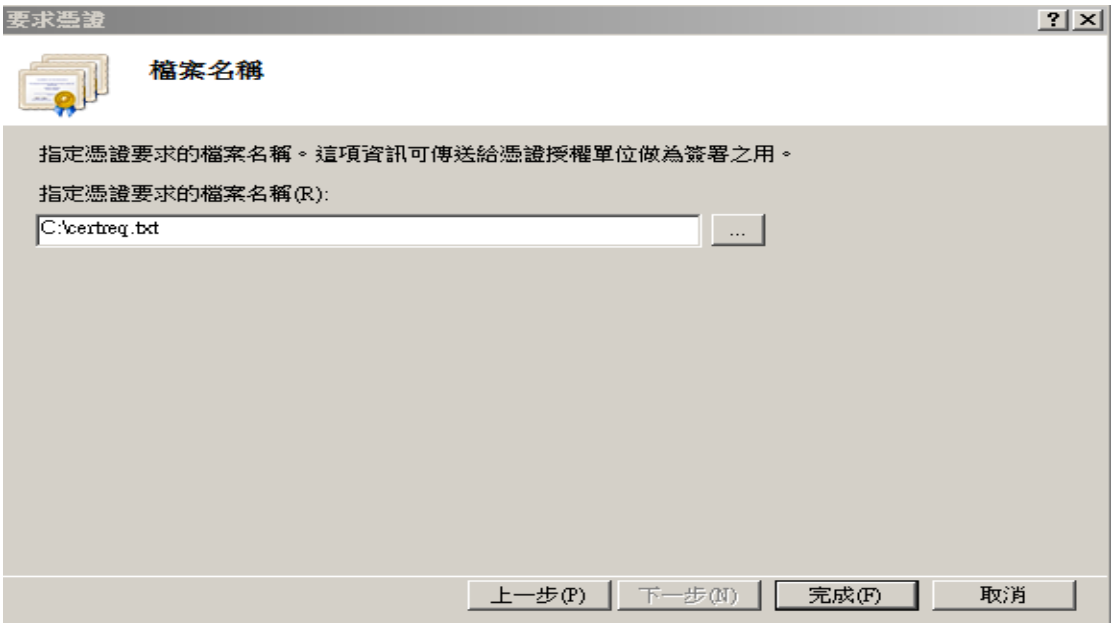
三、輸入以下所有欄位資料，輸入完成後點點選「下一步」



四、選擇密碼編譯服務提供者『Microsoft RSA SChannel Cryptographic Provider』，金鑰長度選擇 『2048』位元。請注意依照國際密碼學趨勢，請使用 RSA 2048 位元(含)以上金鑰長度。



五、指定要儲存憑證請求檔檔案名稱與存放位置，確認後點選「完成」。



六、此時憑證請求檔(certreq.txt)製作完成，使用憑證請求檔至中華電信公開金鑰基礎建設服務網站（https://chtca.hinet.net/）依照網頁說明申請 SSL 憑證。

若屬於中華電信公司各單位申請 SSL 憑證者，請從企業入口網站電子表單之資訊表單「IS14-伺服器應用軟體憑證申請/異動單」提出申請。

補充說明 1: 中華電信公開金鑰基礎建設服務之程式會擷取憑證請求檔中的公開金鑰，但不會使用憑證請求檔中於上圖所輸入之資訊，而是以於申請網頁上所填入的組織資訊與完全吻合網域名稱(Fully Qualified Domain Name, FQDN)為準，並記載於所簽發的 SSL 憑證裡面的欄位[如憑證主體名稱(Subject Name)之一般名稱(Common Name)或憑證主體別名(Subject Alternative Name)等欄位]。

補充說明 2:若您是申請多網域 SSL 憑證或萬用網域 SSL 憑證，僅需要產生 1 個憑證請求檔(產生憑證請求檔之過程就是幫您的伺服器產製 1 對金鑰對，私密金鑰與密碼由伺服器管理者保管，公開金鑰會包含在憑證請求檔內，憑證管理中心審驗您的身分與網域名稱擁有權或控制權後，所簽發的憑證會記載申請者的組織資訊、完全吻合網域名稱與公開金鑰在 SSL 憑證內。後續先安裝 SSL 憑證串鏈於產生憑證請求檔之站台，再將私密金鑰與憑證備份後匯入其他站台，不同廠牌伺服器之匯出與匯入可參考手冊或寫電子郵件給本管理中心技術客服信箱 caservice@cht.com.tw 詢問，不需要每個網站站台都分別產生憑證請求檔。

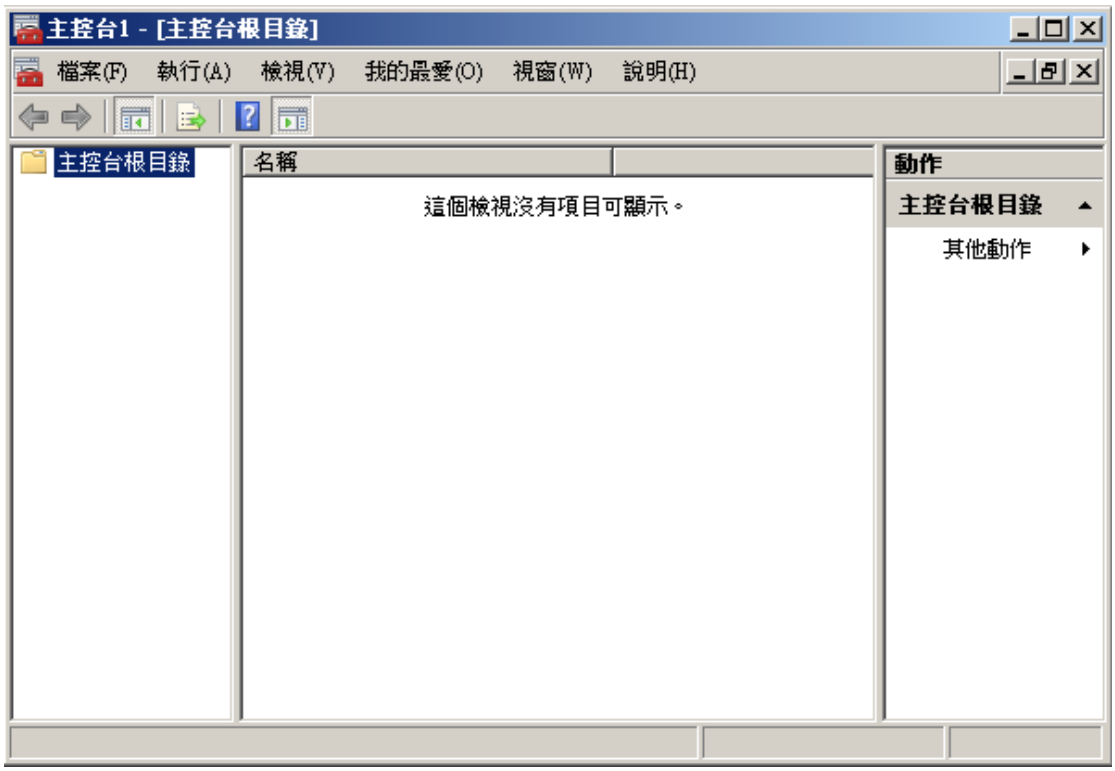
Windows IIS 7.0 SSL 憑證安裝操作手冊

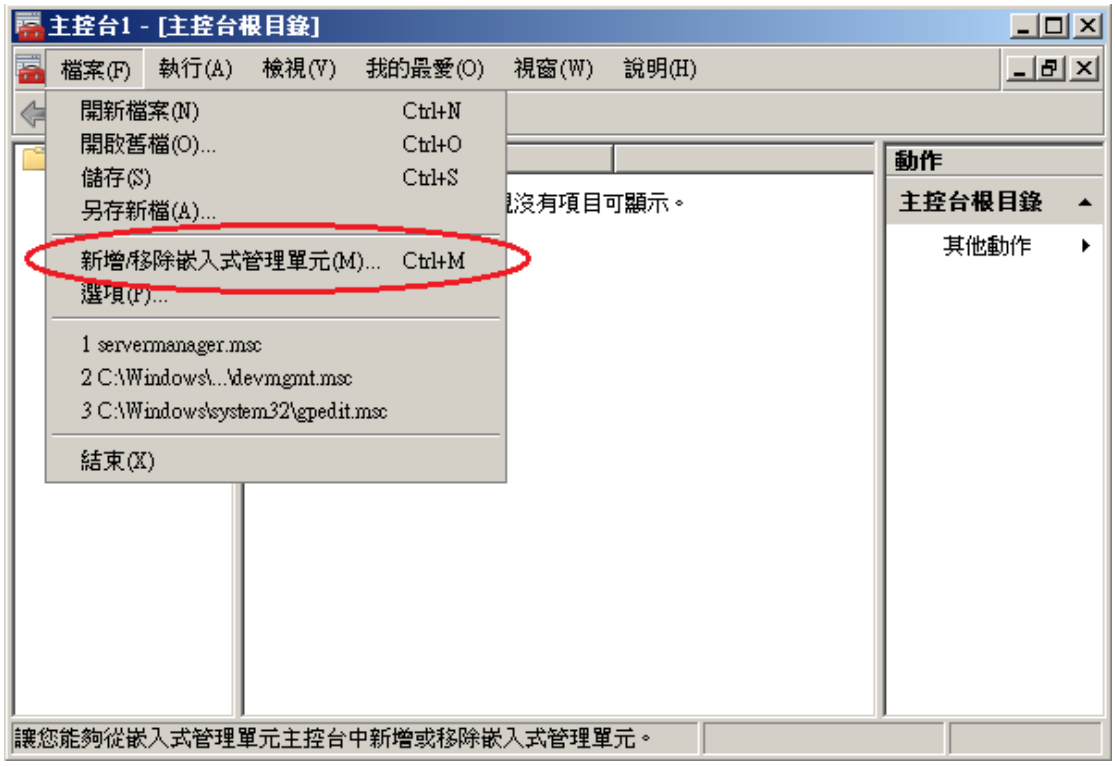
一、下載憑證串鏈，包含 4 張憑證，分別是(1)eCA 根憑證(ePKI Root CA 憑證，也就是中華電信憑證總管理中心自簽憑證)、(2)eCA to HRCA 交互憑證(eCA 簽發給 HRCA 之交互憑證)、(3)HiPKI OV TLS CA 中繼憑證(中華電信 HiPKI OV TLS 憑證管理中心自身憑證)與(4)OV TLS CA 簽發給用戶的 SSL 伺服器憑證，可採以下兩種方式之一取得：

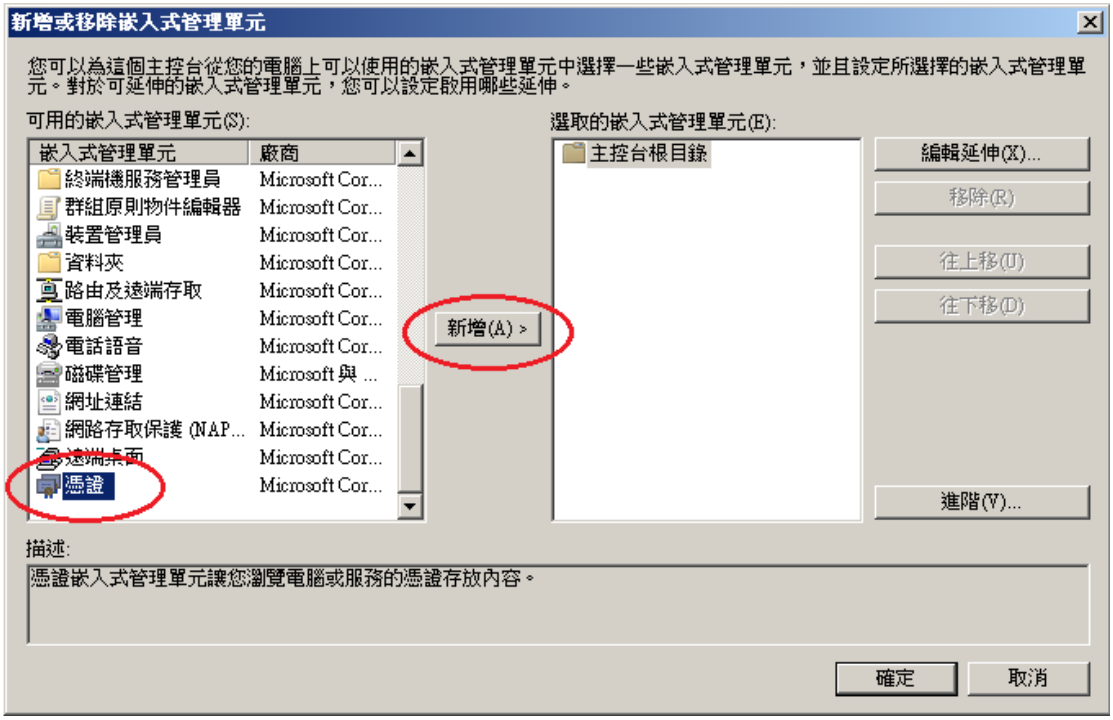
1. 您若是本公司之客戶，技術聯絡人的電子郵件信箱會收到憑證串鏈壓縮檔，解壓縮後包括 4 個檔案，分別是 eCA 根憑證(檔名為 ROOTeCA_64.crt)、eCA to HRCA 交互憑證(檔名為 eCA1-to-HRCA1.crt)、OV TL SCA 中繼憑證(檔名為 OVTLSCA1_b64.crt)與用戶端 SSL 伺服器軟體憑證(檔名為 32 個英數字所組成，此為憑證序號)。
   若是中華電信之所屬單位，於經審驗核准申請之電子表單的資訊表單「IS 14-伺服器應用軟體憑證申請/異動單」頁面下方，可以下載憑證串鏈壓縮檔，解壓縮後可以取得憑證串鏈 4 個檔案。
2. 從網站查詢與下載：
   eCA 憑證：
   https://eca.hinet.net/download/ROOTeCA_64.crt
   eCA to HRCA 憑證：
   https://eca.hinet.net/download/eCA1-to-HRCA1.crt
   HiPKI OV TLS CA 憑證：
   https://eca.hinet.net/repository-h/download/OVTLSCA1_b64.crt
   SSL 憑證下載：您若是本公司之客戶，請至 CHTCA 網站點選「TLS 憑證效期查詢及下載」，進行 SSL 憑證下載。
   若您是中華電信之員工，負責管理單位之伺服器，請至 https://chtra.cht.com.tw/ 點選「憑證與卡片作業」，再點選「憑證查詢」，下載 SSL 憑證。

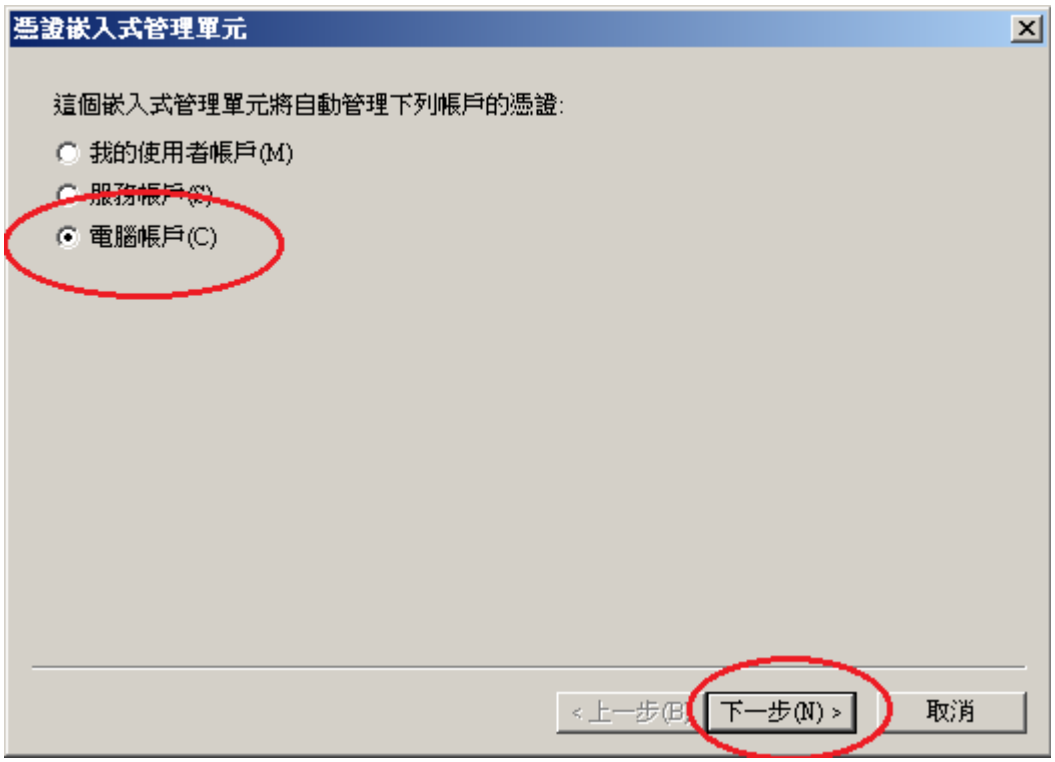
二、開啟 mmc 安裝根憑證及中繼憑證。
點選「開始」→輸入「mmc」→點選「mmc.exe」，並依下圖操作。

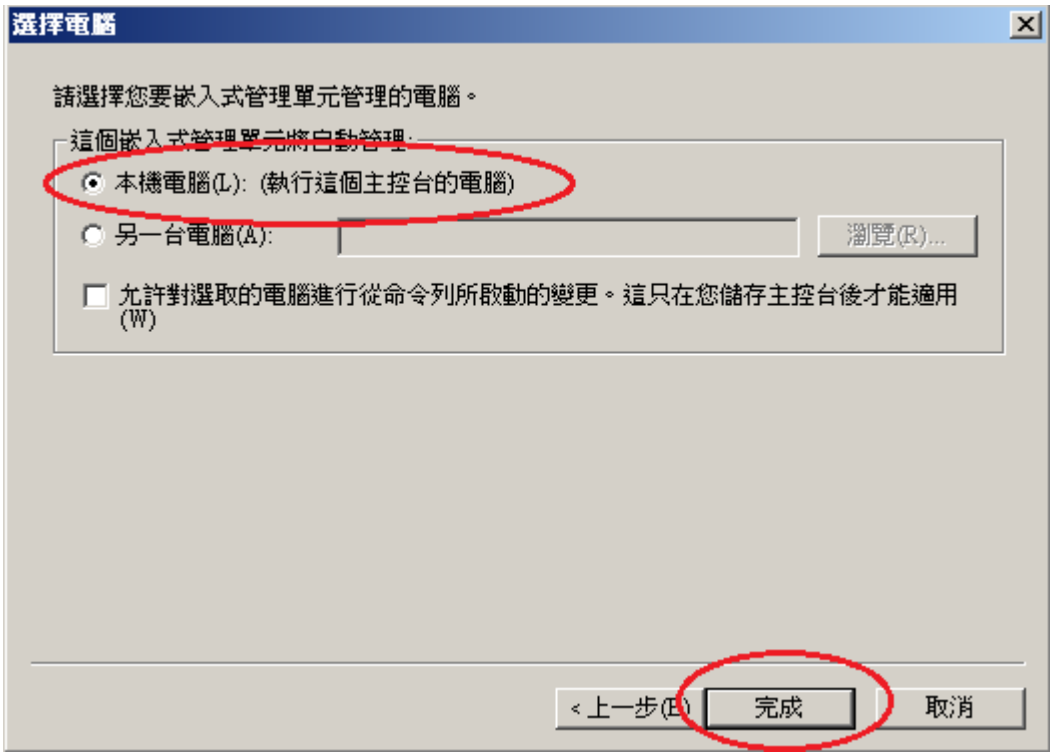

程式集
mmc.exe
檔案
MMC
搜尋每個地方
搜尋網際網路
mmc
開始
Administrator
文件
電腦
網路
控制台
系統管理工具
說明及支援
執行...

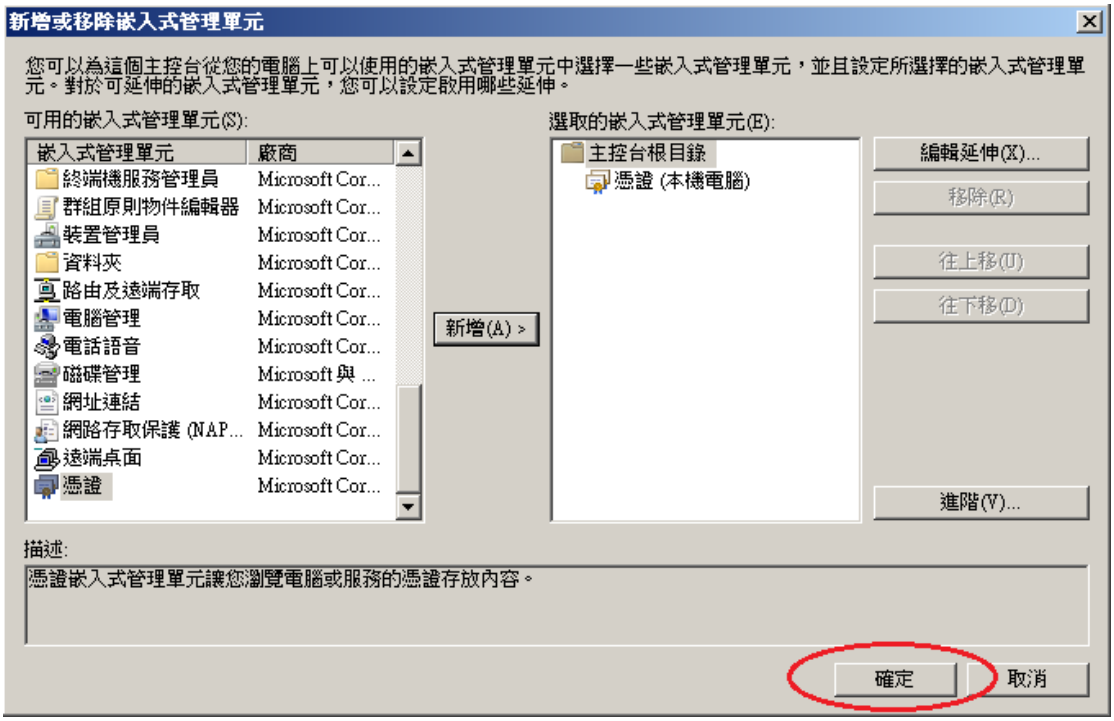

主控台1 - [主控台根目錄]
檔案(F) 執行(A) 檢視(V) 我的最愛(O) 視窗(W) 說明(H)
主控台根目錄
名稱
這個檢視沒有項目可顯示。
動作
主控台根目錄
其他動作


主控台1 - [主控台根目錄]
檔案(F) 執行(A) 檢視(V) 我的最愛(O) 視窗(W) 說明(H)
開新檔案(N) Ctrl+N
開啟舊檔(O)... Ctrl+O
儲存(S) Ctrl+S
另存新檔(A)...
新增/移除嵌入式管理單元(M)... Ctrl+M
選項(P)...
1 servermanager.msc
2 C:\Windows\...\devmgmt.msc
3 C:\Windows\system32\gpedit.msc
結束(X)
沒有項目可顯示。
動作
主控台根目錄
其他動作
讓您能夠從嵌入式管理單元主控台中新增或移除嵌入式管理單元。

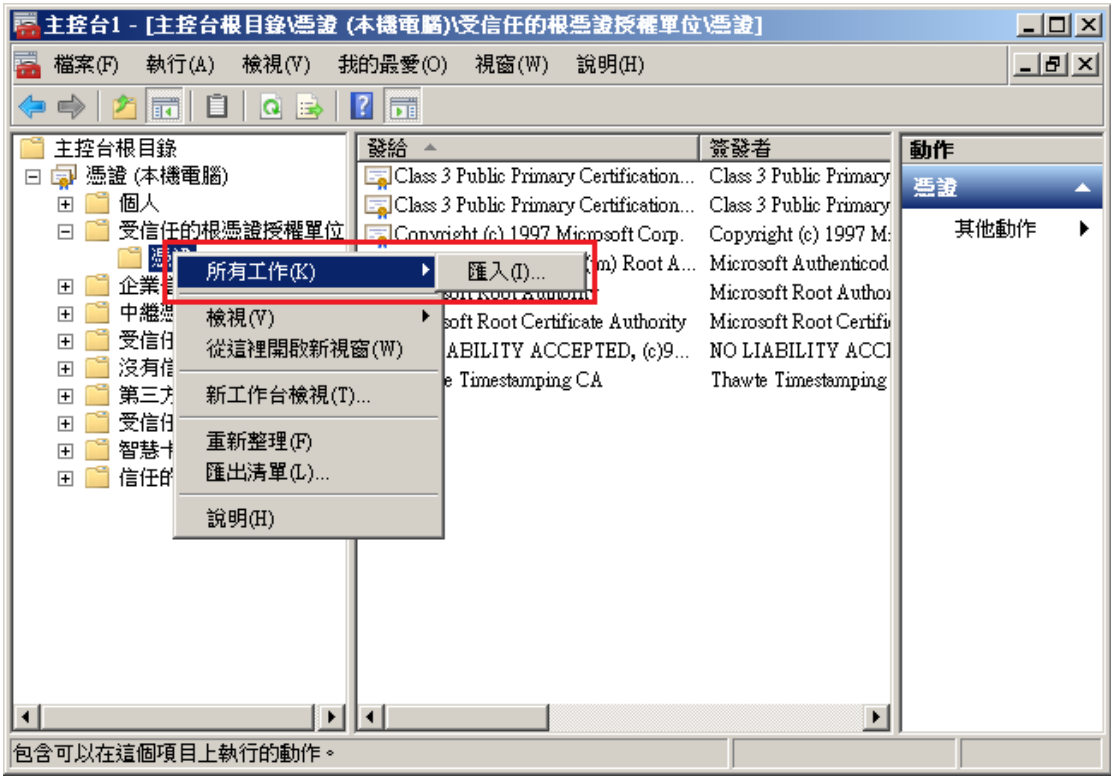

新增或移除嵌入式管理單元
您可以為這個主控台從您的電腦上可以使用的嵌入式管理單元中選擇一些嵌入式管理單元，並且設定所選擇的嵌入式管理單元。對於可延伸的嵌入式管理單元，您可以設定啟用哪些延伸。
可用的嵌入式管理單元(S):
嵌入式管理單元
廠商
終端機服務管理員 Microsoft Cor...
群組原則物件編輯器 Microsoft Cor...
裝置管理員 Microsoft Cor...
資料夾 Microsoft Cor...
路由及遠端存取 Microsoft Cor...
電腦管理 Microsoft Cor...
電話語音 Microsoft Cor...
磁碟管理 Microsoft 與 ...
網址連結 Microsoft Cor...
網路存取保護 (NAP... Microsoft Cor...
遠端桌面 Microsoft Cor...
憑證 Microsoft Cor...
新增(A) >
選取的嵌入式管理單元(E):
主控台根目錄
編輯延伸(X)...
移除(R)
往上移(U)
往下移(D)
進階(V)...
描述:
憑證嵌入式管理單元讓您瀏覽電腦或服務的憑證存放內容。
確定
取消

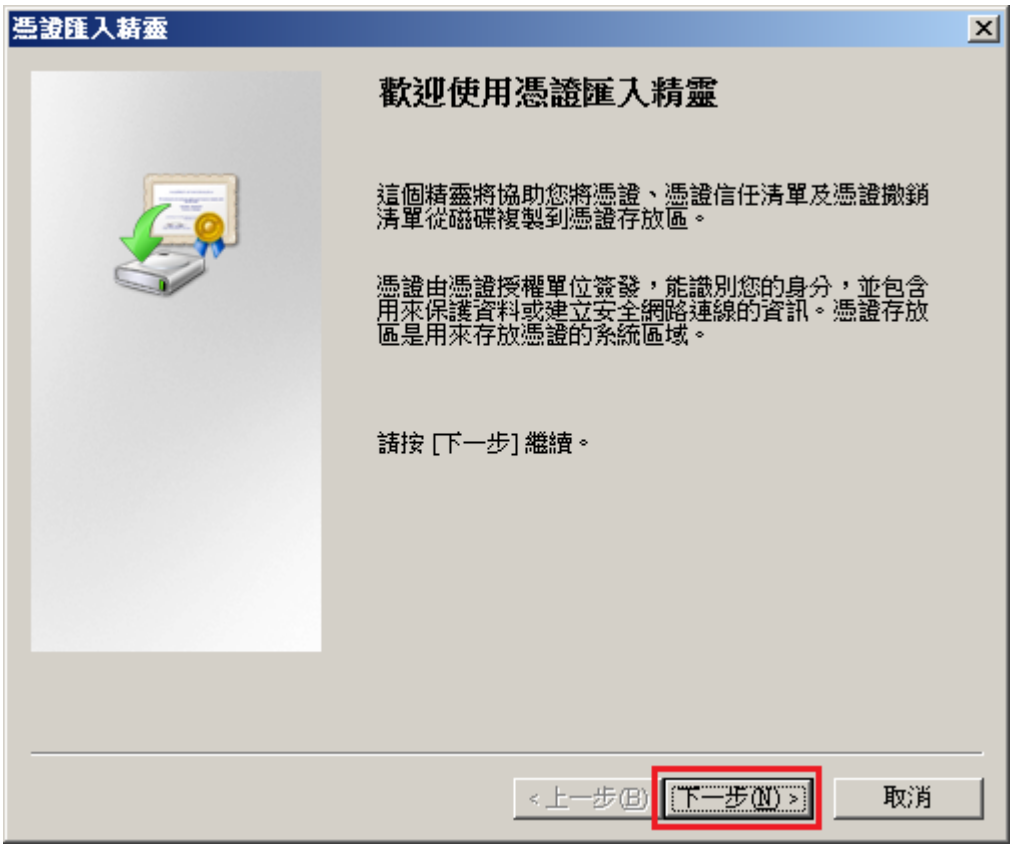

憑證嵌入式管理單元
這個嵌入式管理單元將自動管理下列帳戶的憑證:
我的使用者帳戶(M)
服務帳戶(S)
電腦帳戶(C)
< 上一步(B)
下一步(N) >
取消

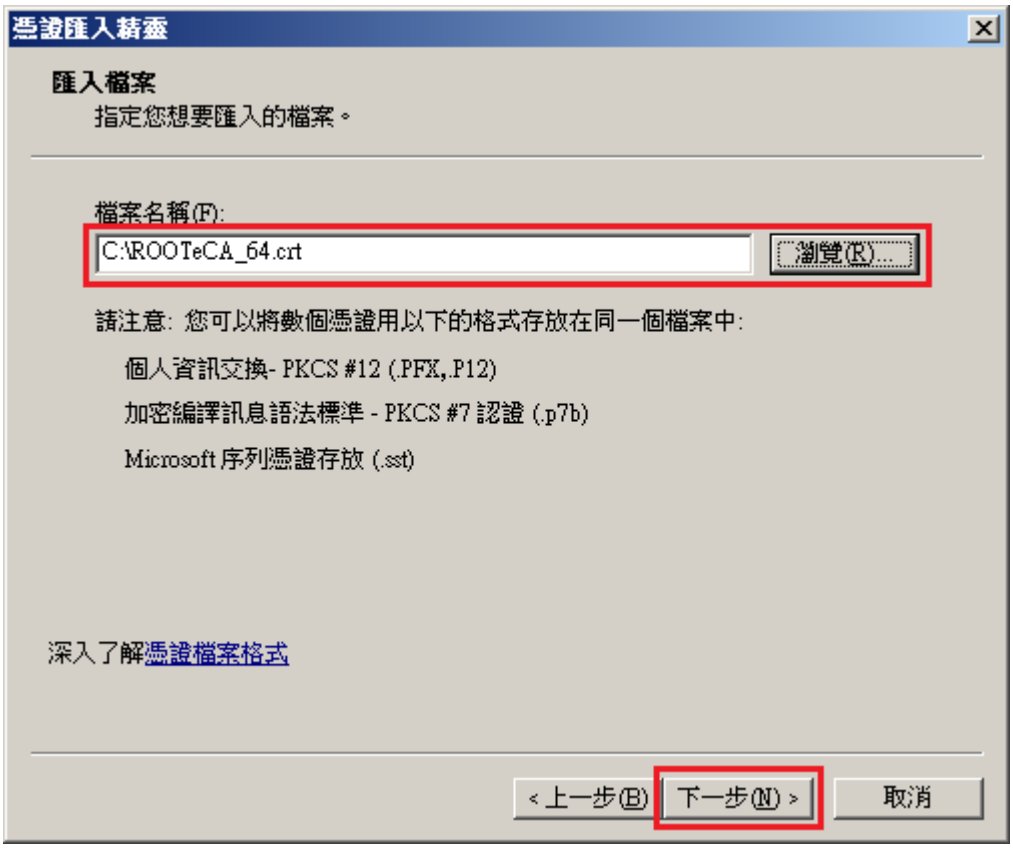


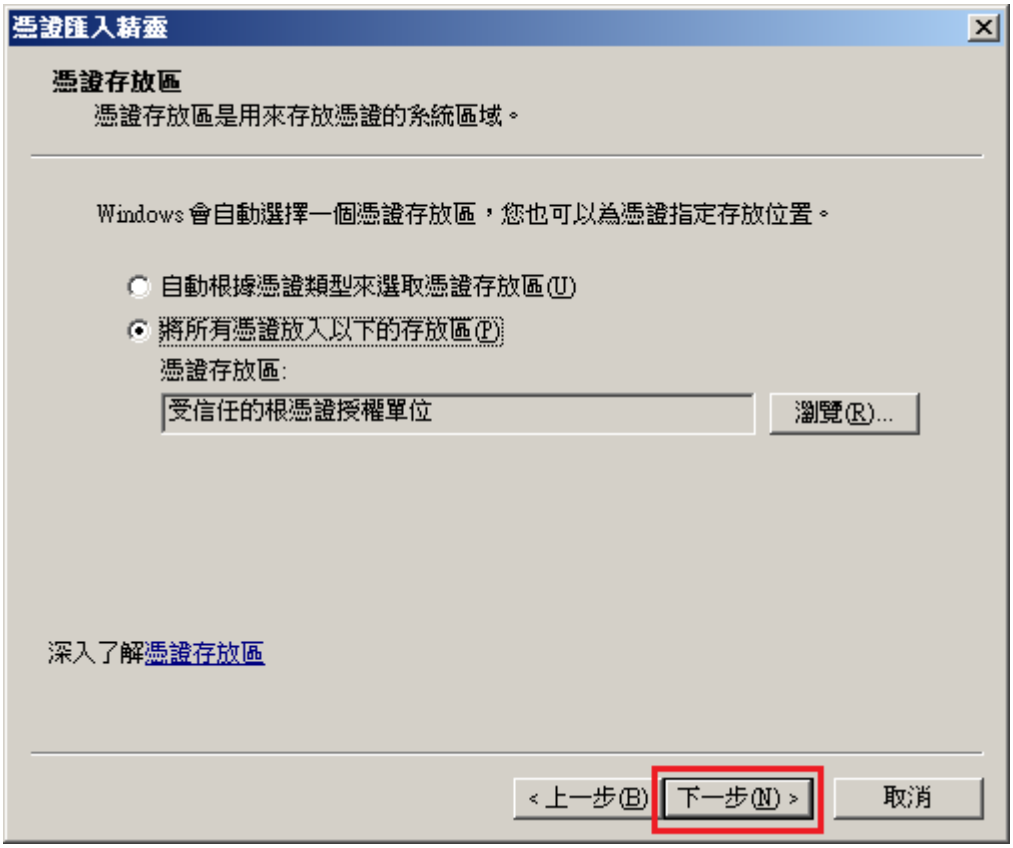


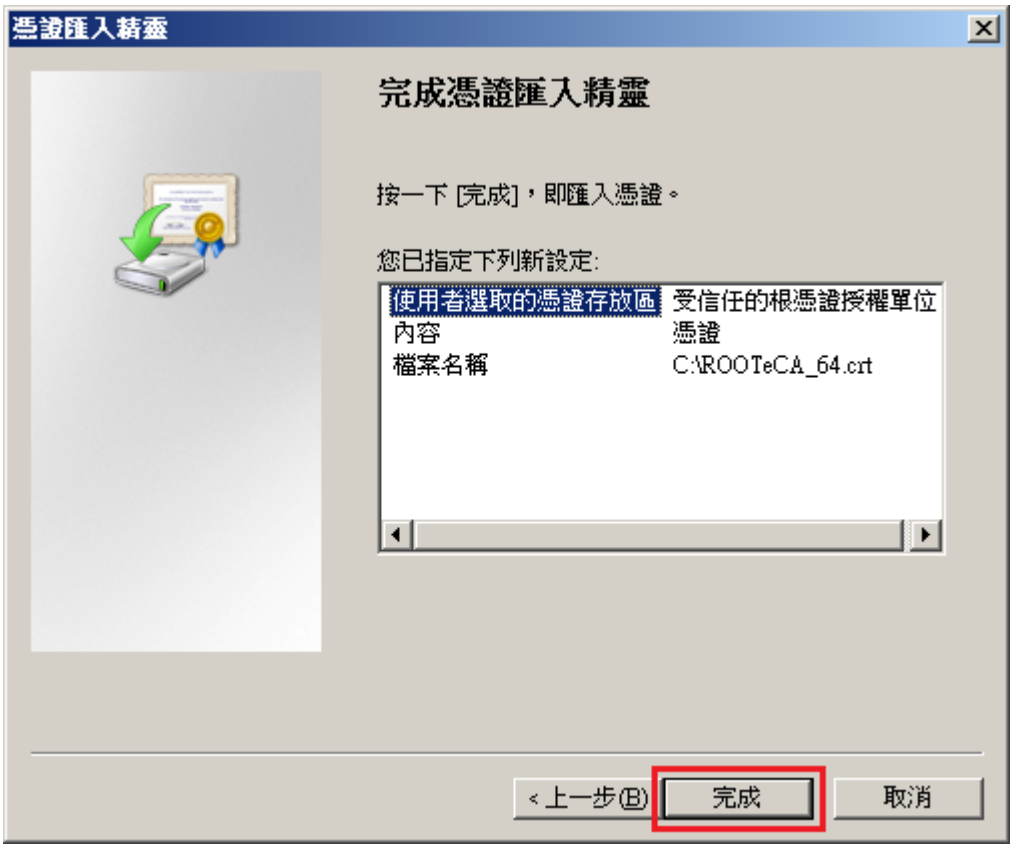
三、於「受信任的根憑證授權單位」匯入根憑證。


主控台1 - [主控台根目錄\憑證 (本機電腦)\受信任的根憑證授權單位\憑證]
檔案(F) 執行(A) 檢視(V) 我的最愛(O) 視窗(W) 說明(H)
主控台根目錄
憑證 (本機電腦)
個人
受信任的根憑證授權單位
企業
中繼
受信任
沒有信
第三方
受信任
智慧卡
信任的
發給
簽發者
Class 3 Public Primary Certification...
Class 3 Public Primary Certification...
Copyright (c) 1997 Microsoft Corp.
Root A...
Microsoft Root Authority
ABILITY ACCEPTED, (c)9...
Timestamping CA
Class 3 Public Primary
Class 3 Public Primary
Copyright (c) 1997 M
Microsoft Authenticod
Microsoft Root Autho
Microsoft Root Certifi
NO LIABILITY ACCI
Thawte Timestamping
動作
憑證
其他動作
所有工作(K)
匯入(I)...
檢視(V)
從這裡開啟新視窗(W)
新工作台檢視(T)...
重新整理(F)
匯出清單(L)...
說明(H)
包含可以在這個項目上執行的動作。

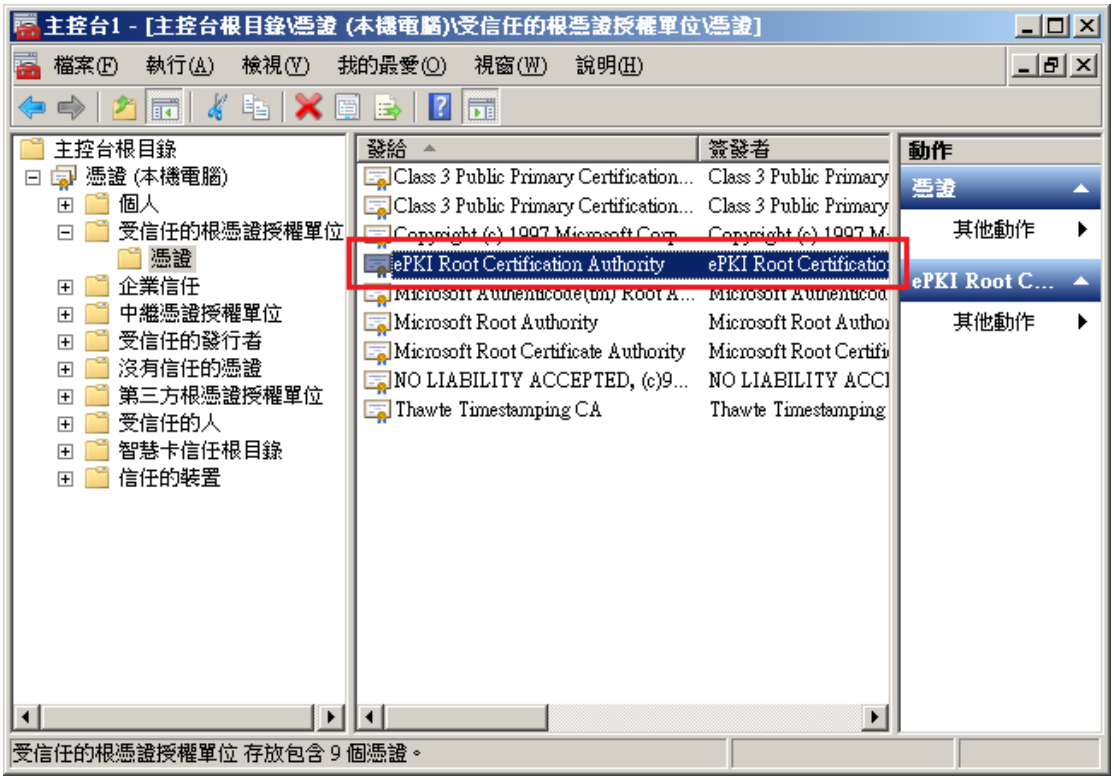

憑證匯入精靈
歡迎使用憑證匯入精靈
這個精靈將協助您將憑證、憑證信任清單及憑證撤銷清單從磁碟複製到憑證存放區。
憑證由憑證授權單位簽發，能識別您的身分，並包含用來保護資料或建立安全網路連線的資訊。憑證存放區是用來存放憑證的系統區域。
請按 [下一步] 繼續。
< 上一步(B)
下一步(N) >
取消


憑證匯入精靈
匯入檔案
指定您想要匯入的檔案。
檔案名稱(F):
C:\ROOTeCA_64.crt
瀏覽(R)...
請注意: 您可以將數個憑證用以下的格式存放在同一個檔案中:
個人資訊交換- PKCS #12 (.PFX,.P12)
加密編譯訊息語法標準 - PKCS #7 認證 (.p7b)
Microsoft 序列憑證存放 (.sst)
深入了解憑證檔案格式
< 上一步(B)
下一步(N) >
取消

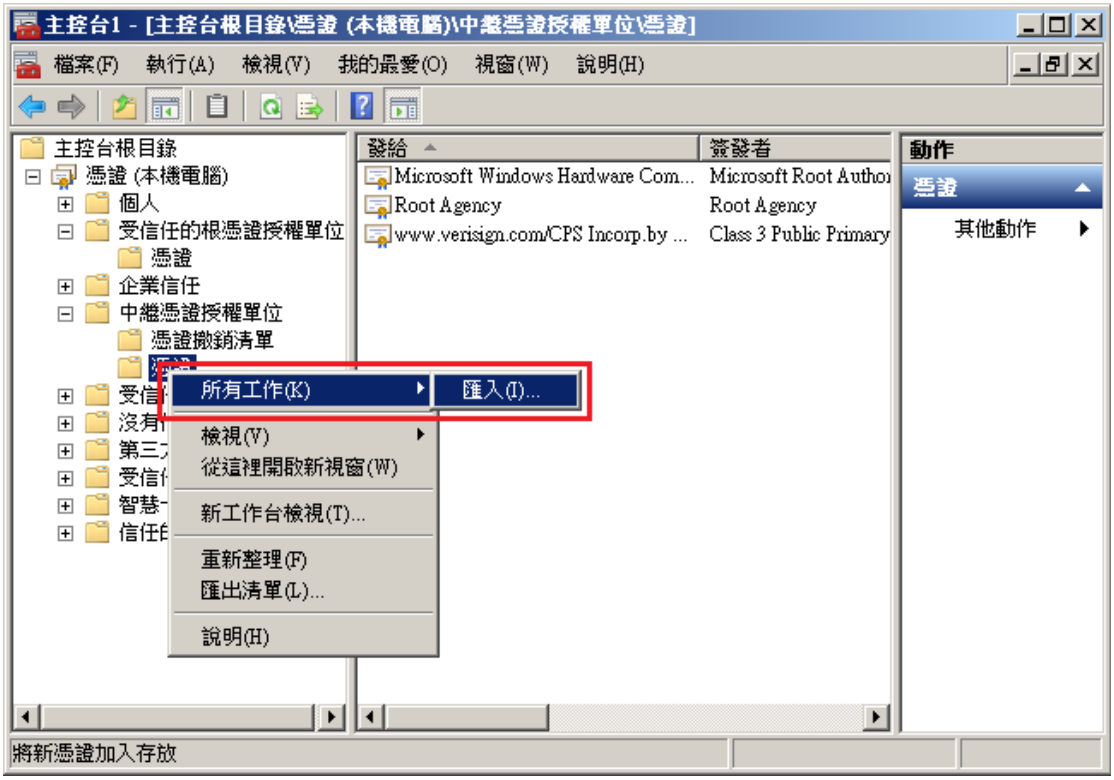

憑證匯入精靈
憑證存放區
憑證存放區是用來存放憑證的系統區域。
Windows 會自動選擇一個憑證存放區，您也可以為憑證指定存放位置。
自動根據憑證類型來選取憑證存放區(U)
將所有憑證放入以下的存放區(P)
憑證存放區:
受信任的根憑證授權單位
瀏覽(R)...
深入了解憑證存放區
< 上一步(B)
下一步(N) >
取消

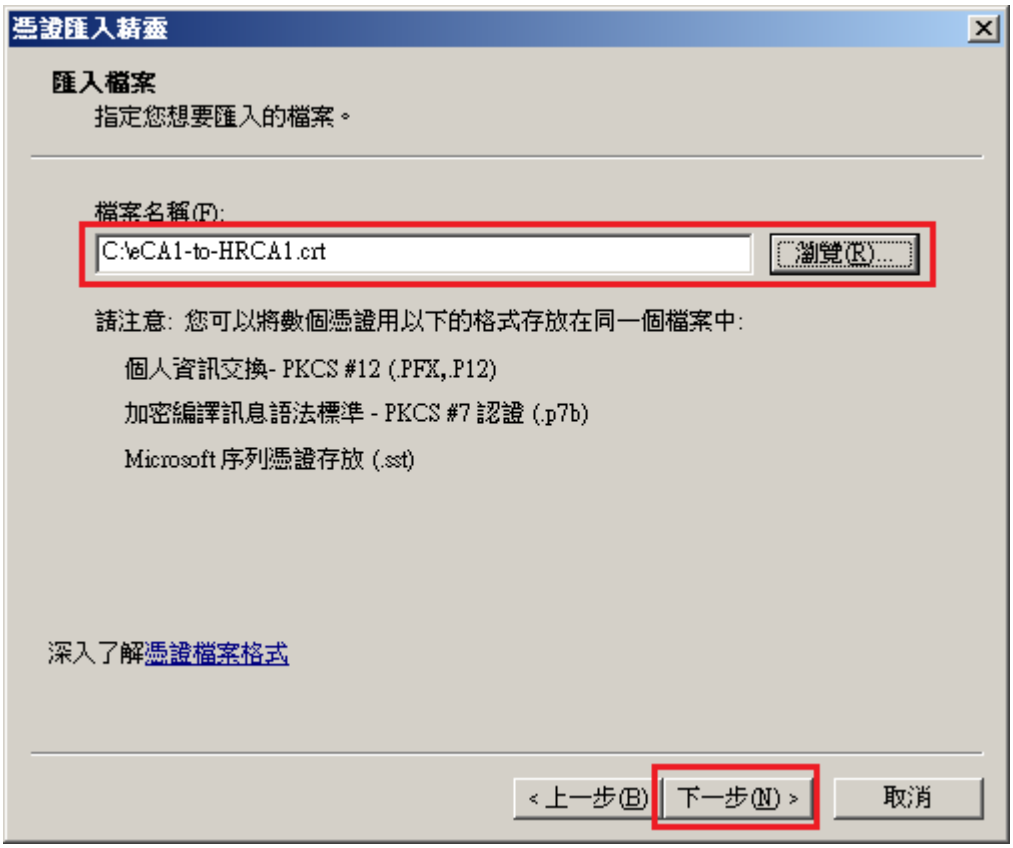

憑證匯入精靈
完成憑證匯入精靈
按一下 [完成]，即匯入憑證。
您已指定下列新設定:
使用者選取的憑證存放區
受信任的根憑證授權單位
內容
憑證
檔案名稱
C:\ROOTeCA_64.crt
< 上一步(B)
完成
取消


憑證匯入精靈
匯入執行成功。
確定

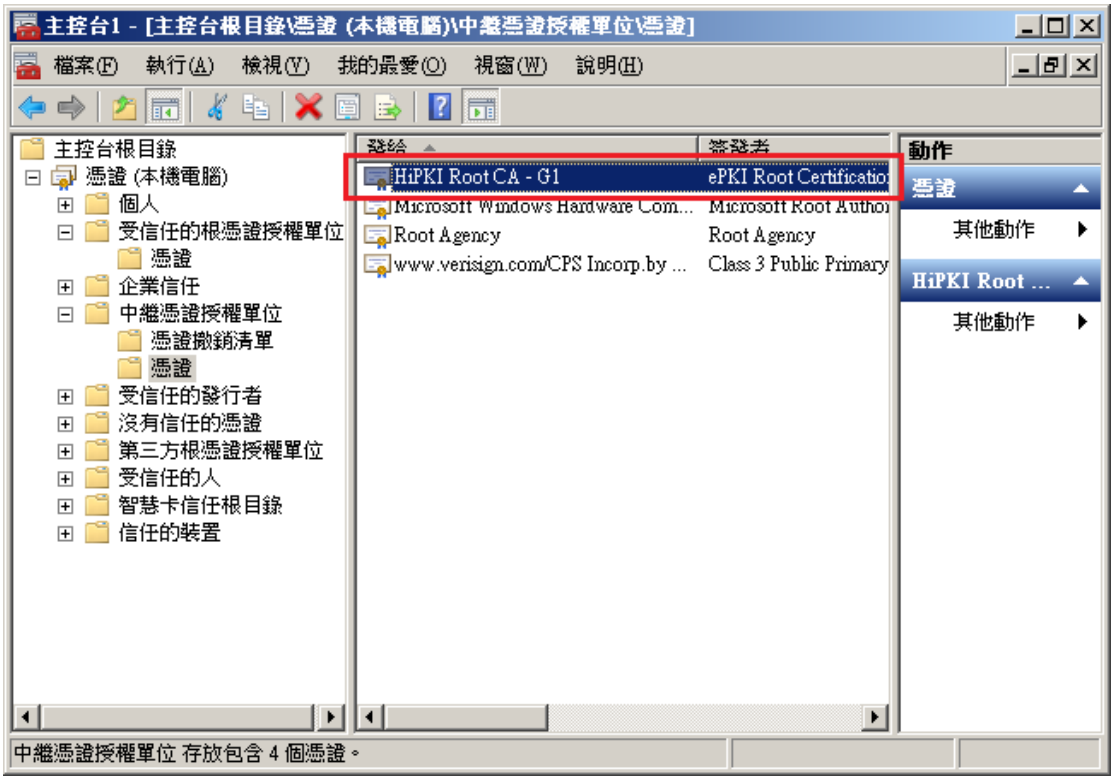


四、於「中繼憑證授權單位」匯入交互憑證。依照上述匯入根憑證的步驟，匯入交互憑證。

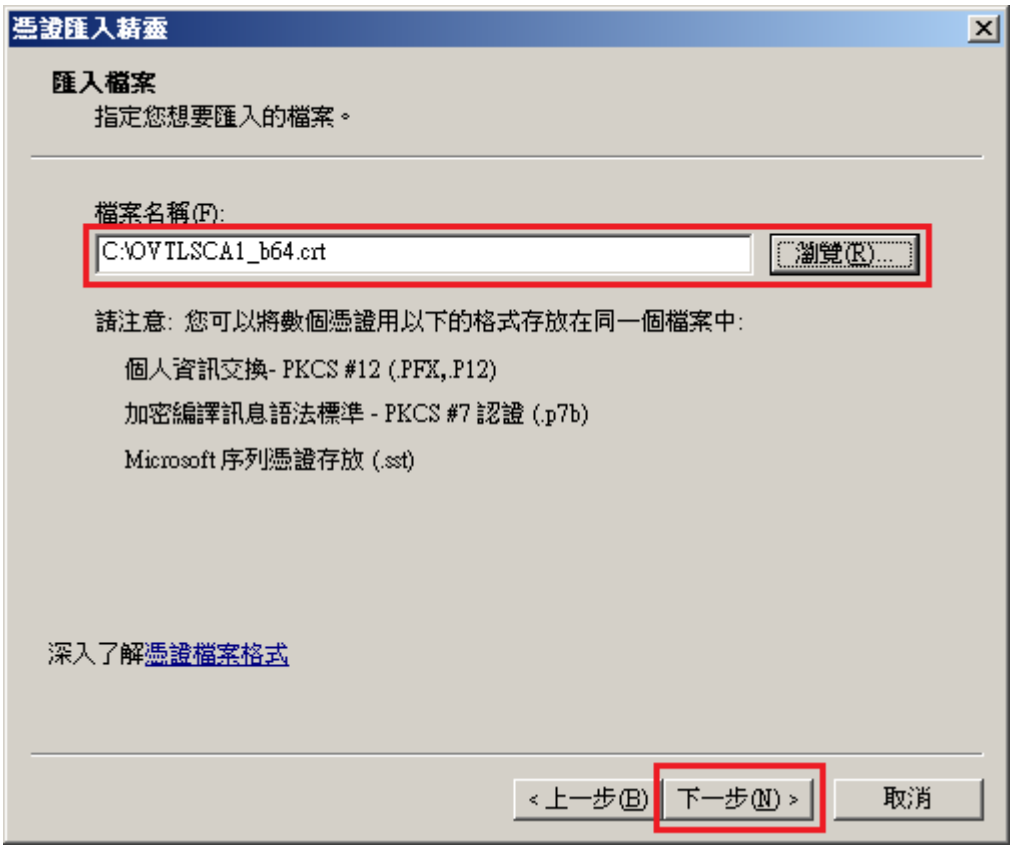


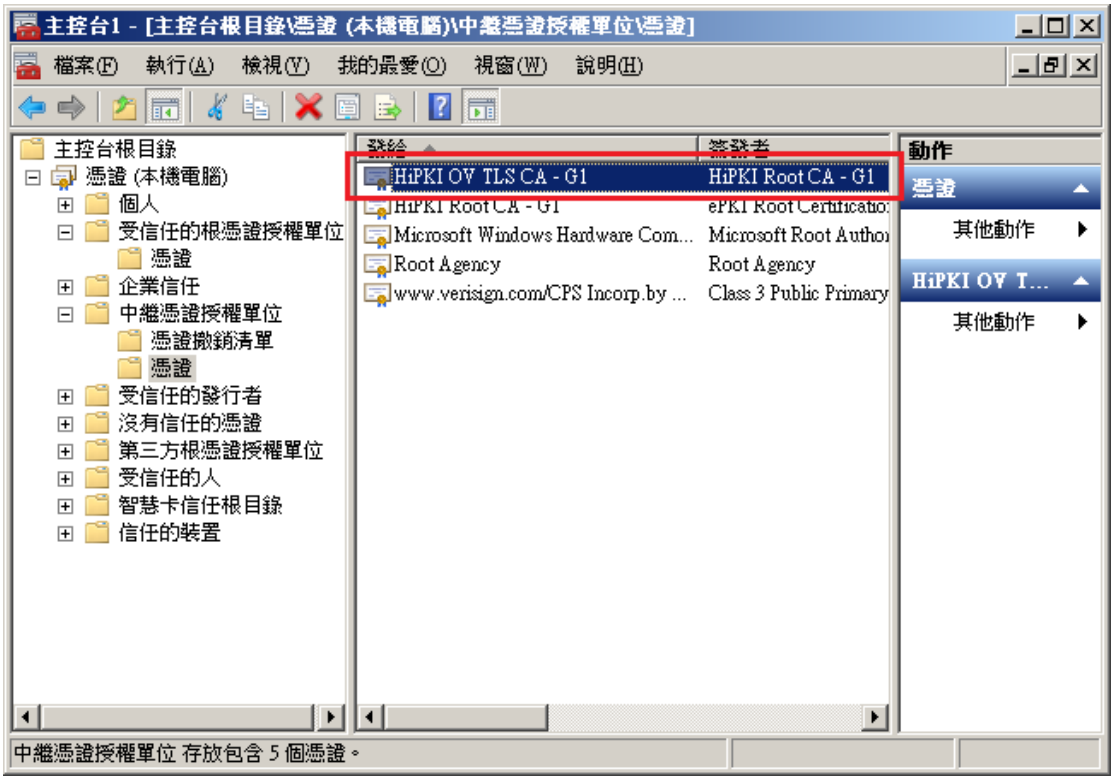

憑證匯入精靈
匯入檔案
指定您想要匯入的檔案。
檔案名稱(F):
C:\eCA1-to-HRCA1.crt
瀏覽(R)...
請注意: 您可以將數個憑證用以下的格式存放在同一個檔案中:
個人資訊交換- PKCS #12 (.PFX,.P12)
加密編譯訊息語法標準 - PKCS #7 認證 (.p7b)
Microsoft 序列憑證存放 (.sst)
深入了解憑證檔案格式
< 上一步(B)
下一步(N) >
取消


憑證匯入精靈
完成憑證匯入精靈
按一下 [完成]，即匯入憑證。
您已指定下列新設定:
使用者選取的憑證存放區
中繼憑證授權單位
內容
憑證
檔案名稱
C:\eCA1-to-HRCA1.crt
< 上一步(B)
完成
取消

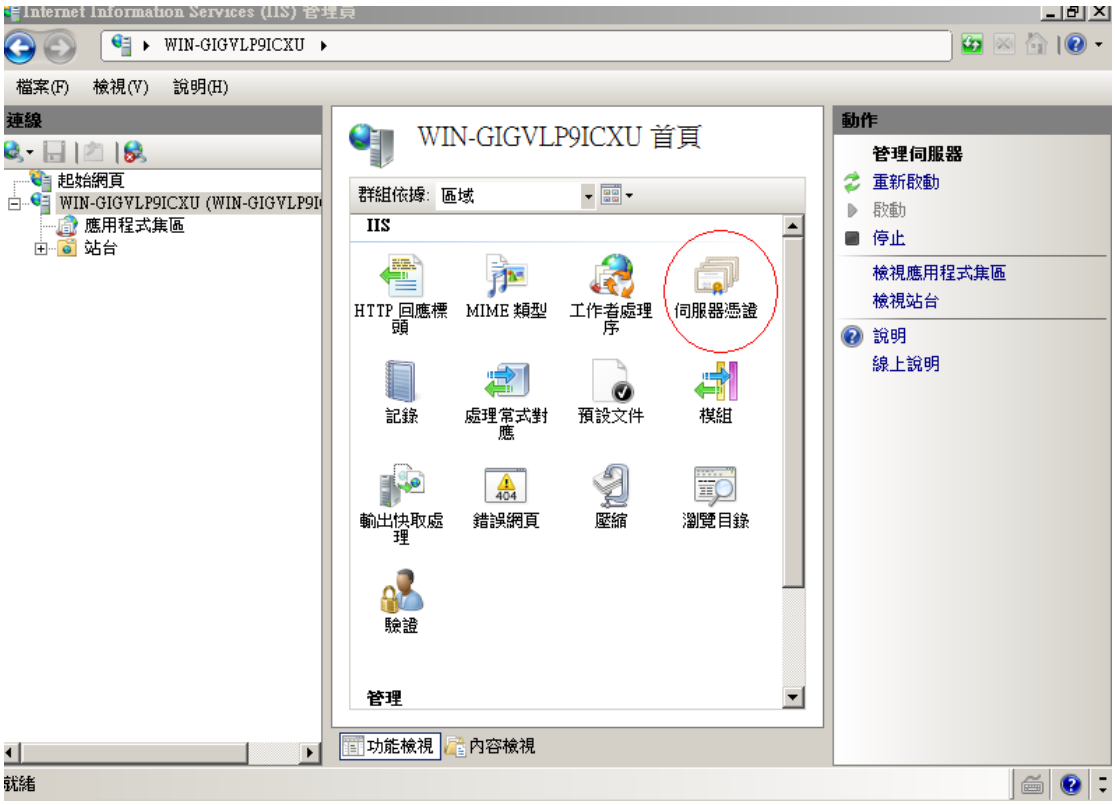


五、於「中繼憑證授權單位」匯入中繼憑證。依照上述匯入根憑證的步驟，匯入中繼憑證。

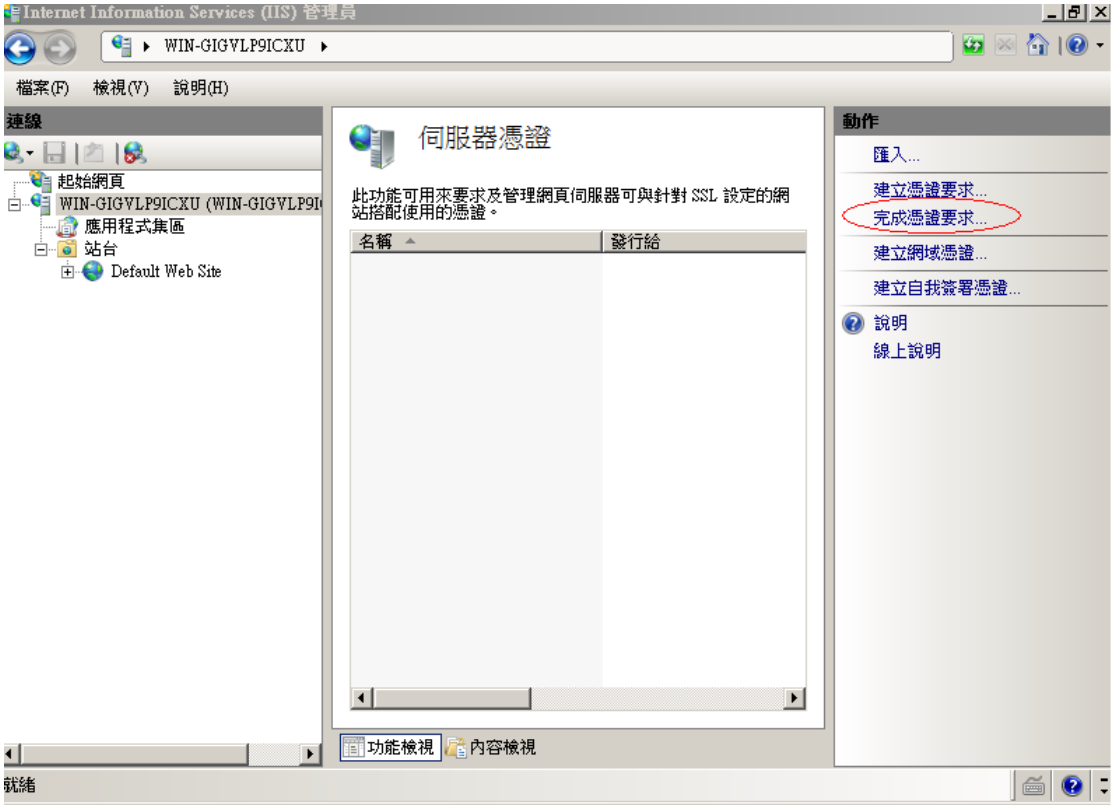




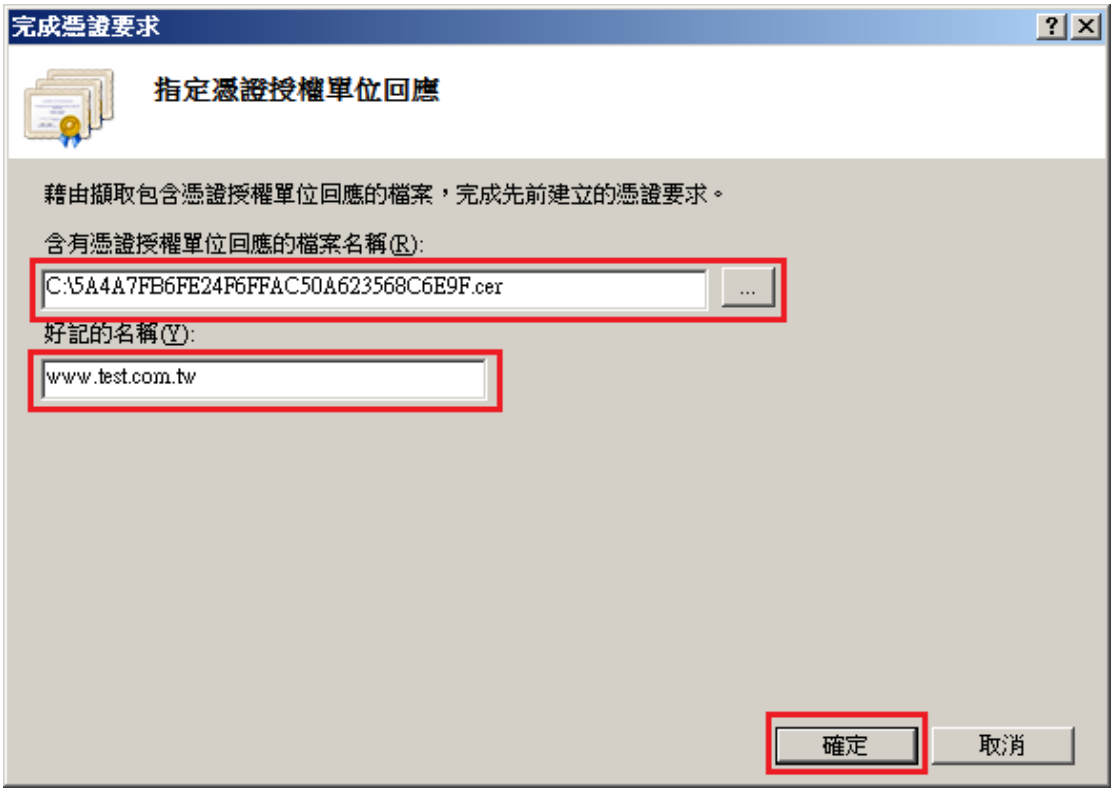
六、開啟「Internet Information Services (IIS)管理員」，點選主機連線預設名稱，再點選畫面右邊「伺服器憑證」。



七、點選「完成憑證要求」。



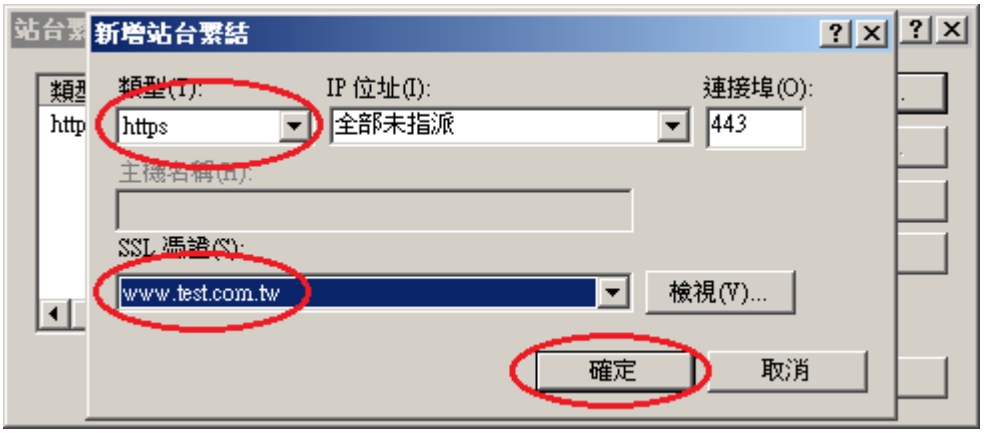
八、選擇由憑證管理中心所簽發之 SSL 憑證路徑，並輸入好記名稱(範例填寫 Domain Name)。



九、伺服器憑證出現匯入的憑證項目。

十、點選要安裝的站台，本手冊以(Default Web Site)進行說明，選擇「繫結」→ 新增→類型『https』、連接埠 『443』，選擇要安裝在此站台之 SSL 憑證

(www.test.com.tw) 。



十一、 依照您的網路架構，您可能需要於防火牆開啟對應 https 的 port。

十二、 安裝 SSL 安全認證標章

請用戶參考技術聯絡人的電子郵件信箱所收到 SSL 憑證串鏈電子郵件內文的 SSL 安全認證標章安裝說明，將網站 SSL 安全認證標章安裝成功，網友可瀏覽您所維護網站所安裝 SSL 憑證的狀態與資訊。

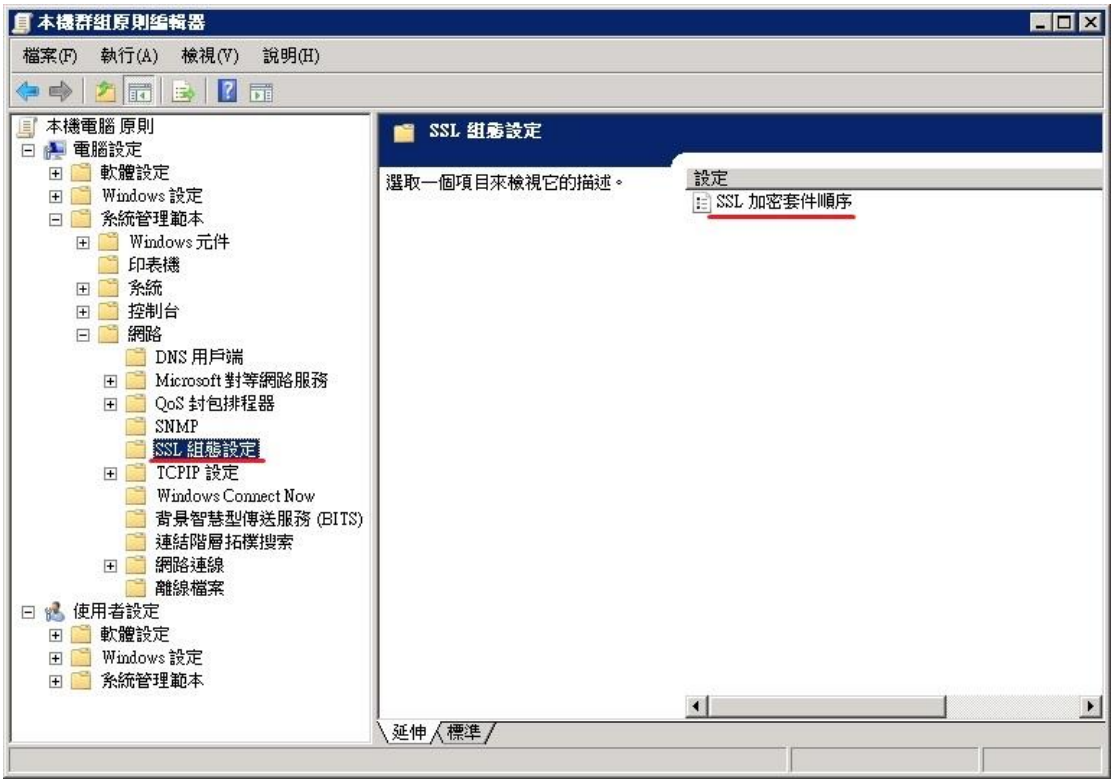
請中華電信公司負責維護網站的同仁，參考從企業入口網站電子表單之資訊表單「IS14-伺服器應用軟體憑證申請/異動單」所下載 SSL 憑證串鏈檔案中的 SSLSealispec.txt，將網站 SSL 安全認證標章安裝成功。

附件一：設定 SSL 安全通道的加密強度

IIS 7.0 預設使用 AES 128 位元來進行資料加密，欲使用 AES 256 位元來進行資料加密的話，可以參考以下步驟：

一、啟動 gpedit.msc 程式

二、選擇 SSL 組態設定，對著「SSL 加密套件順序」點兩下。



三、選擇「已啟用」，並修改 SSL 加密套件的欄位。

原加密套件順序：

TLS_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_AES_256_CBC_SHA,TLS_RSA_WITH_RC4_128_SHA,TLS_RSA_WITH_3DES_EDE_CBC_SHA,TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA_P256,TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA_P384,TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA_P521,TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA_P256,TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA_P384,TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA_P521,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P256,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P384,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P521,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA_P256,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA_P384,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA_P521,TLS_DHE_DSS_WITH_AES_128_CBC_SHA,TLS_DHE_DSS_WITH_AES_256_CBC_SHA,TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA,TLS_RSA_WITH_RC4_128_MD5,SSL_CK_RC4_128_WITH_MD5,SSL_CK_DES_192_EDE3_CBC_WITH_MD5,TLS_RSA_WITH_NULL_MD5,TLS_RSA_WITH_NULL_SHA

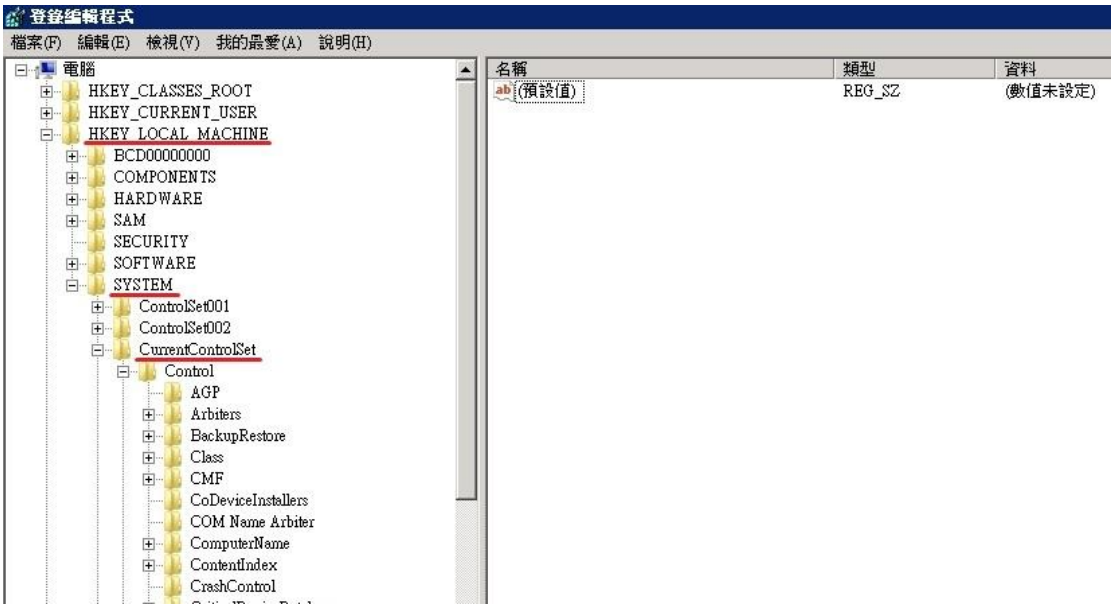
修改後的加密套件順序：

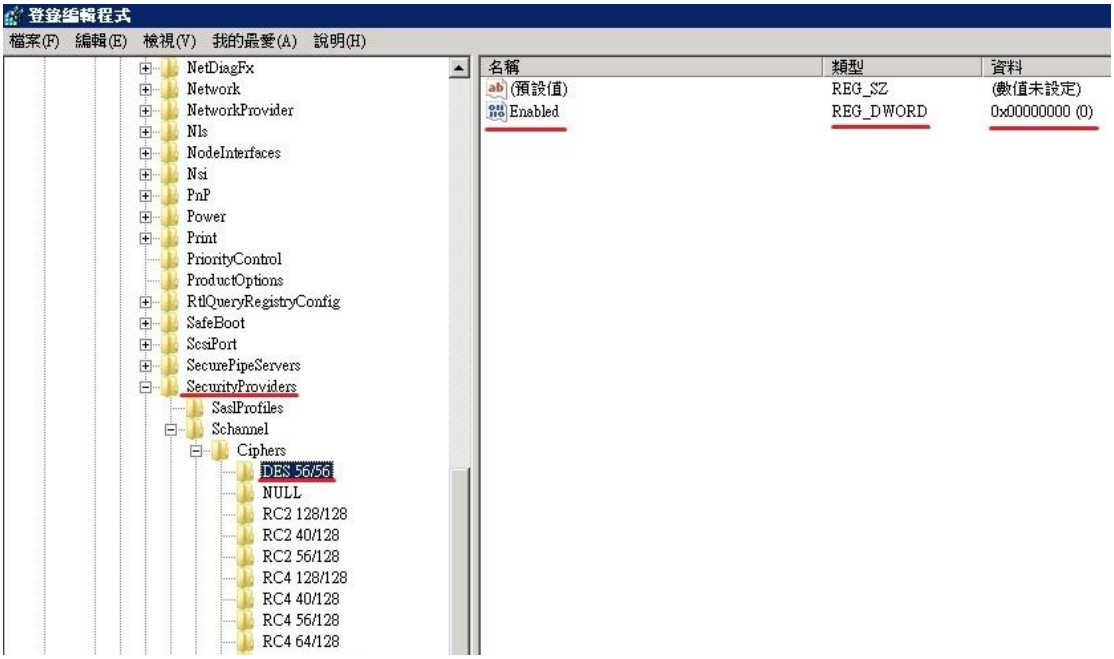
TLS_RSA_WITH_AES_256_CBC_SHA,TLS_RSA_WITH_RC4_128_SHA,TLS_RSA_WITH_3DES_EDE_CBC_SHA,TLS_ECDHE_ECDSA_WITH_AES

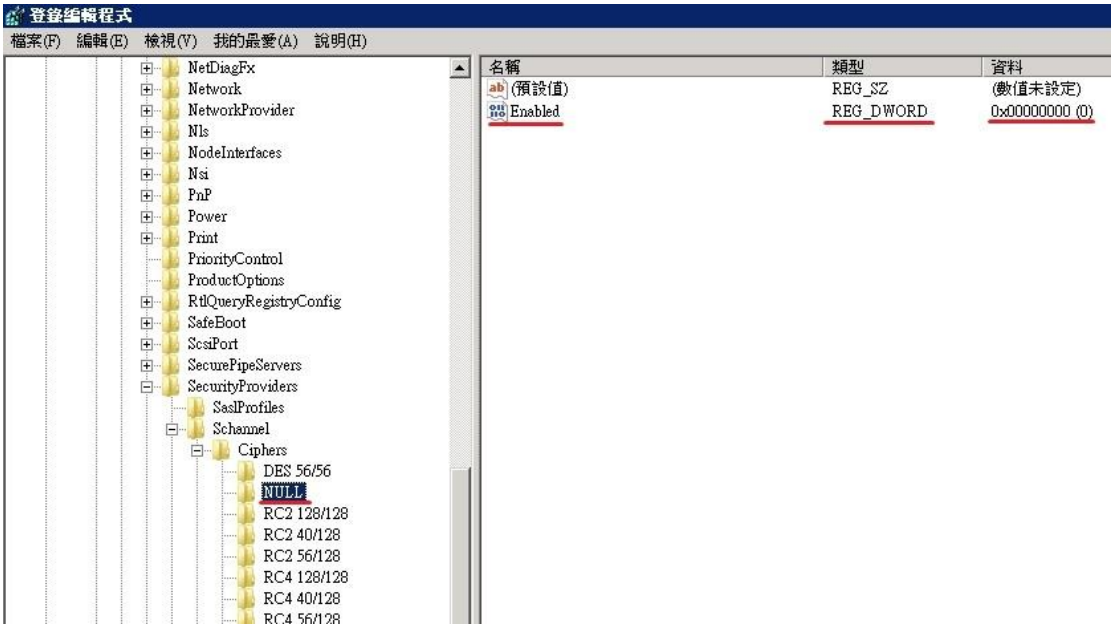
_128_CBC_SHA_P256,TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA_P384,TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA_P521,TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA_P256,TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA_P384,TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA_P521,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P256,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P384,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P521,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA_P256,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA_P384,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA_P521,TLS_DHE_DSS_WITH_AES_128_CBC_SHA,TLS_DHE_DSS_WITH_AES_256_CBC_SHA,TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA,TLS_RSA_WITH_RC4_128_MD5,SSL_CK_RC4_128_WITH_MD5,SSL_CK_DES_192_EDE3_CBC_WITH_MD5,TLS_RSA_WITH_NULL_MD5,TLS_RSA_WITH_NULL_SHA

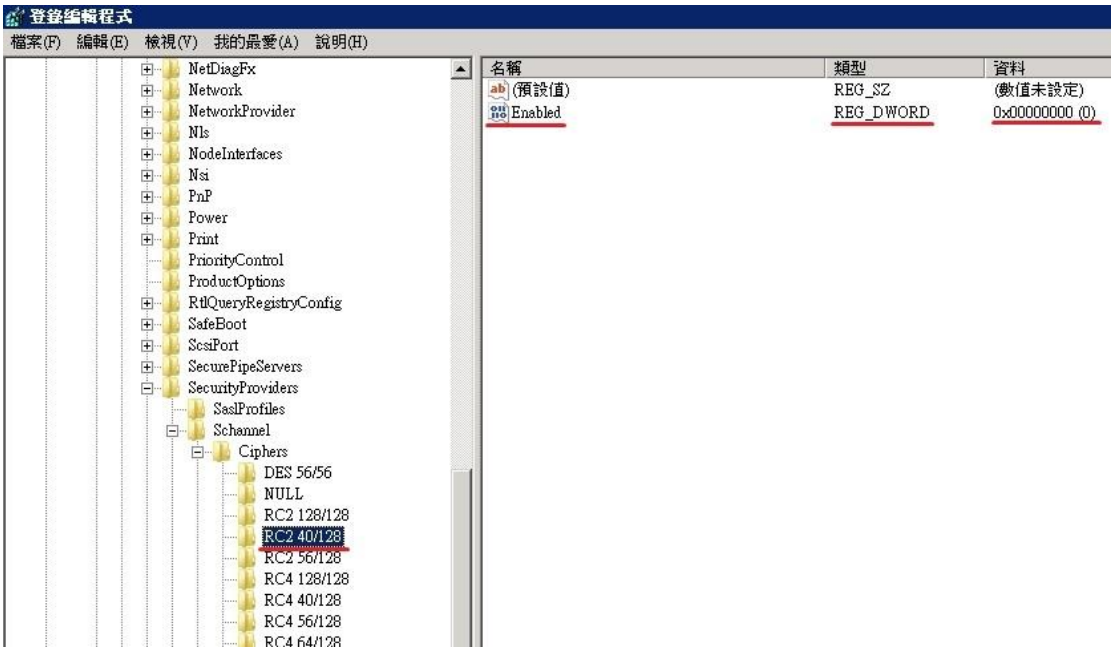
四、開啟登錄檔編輯程式。

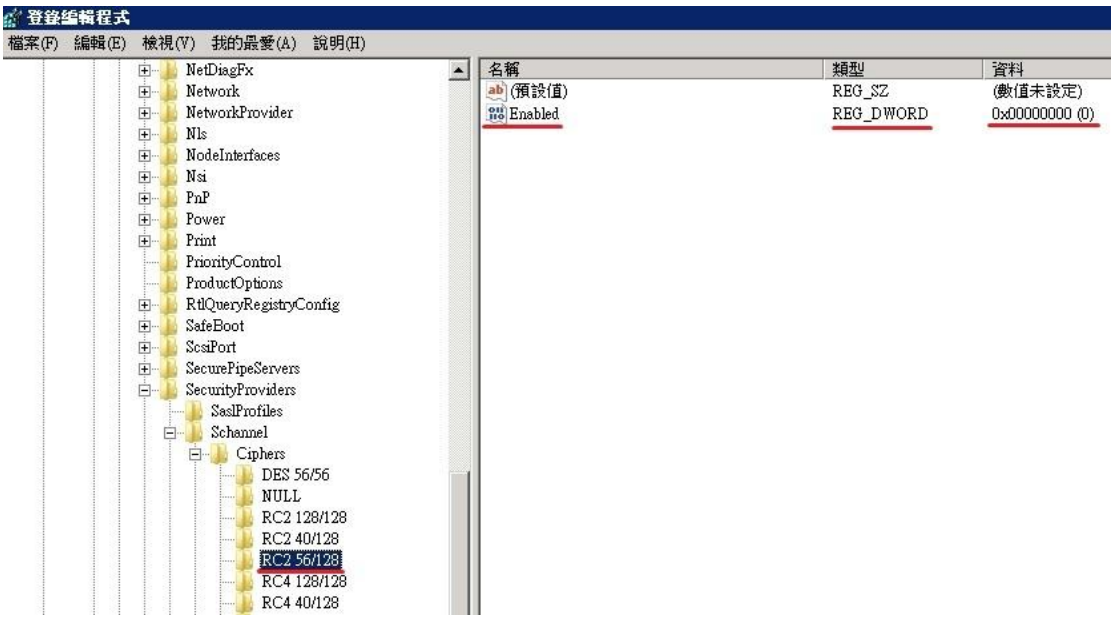
五、依照下圖進行登錄檔編輯。

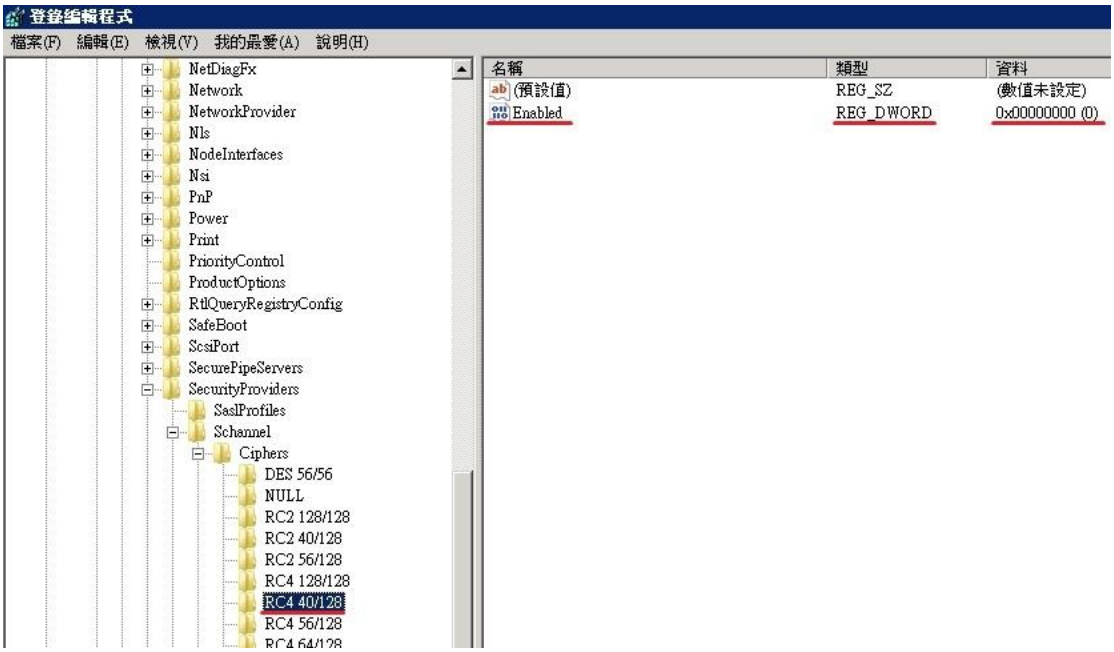


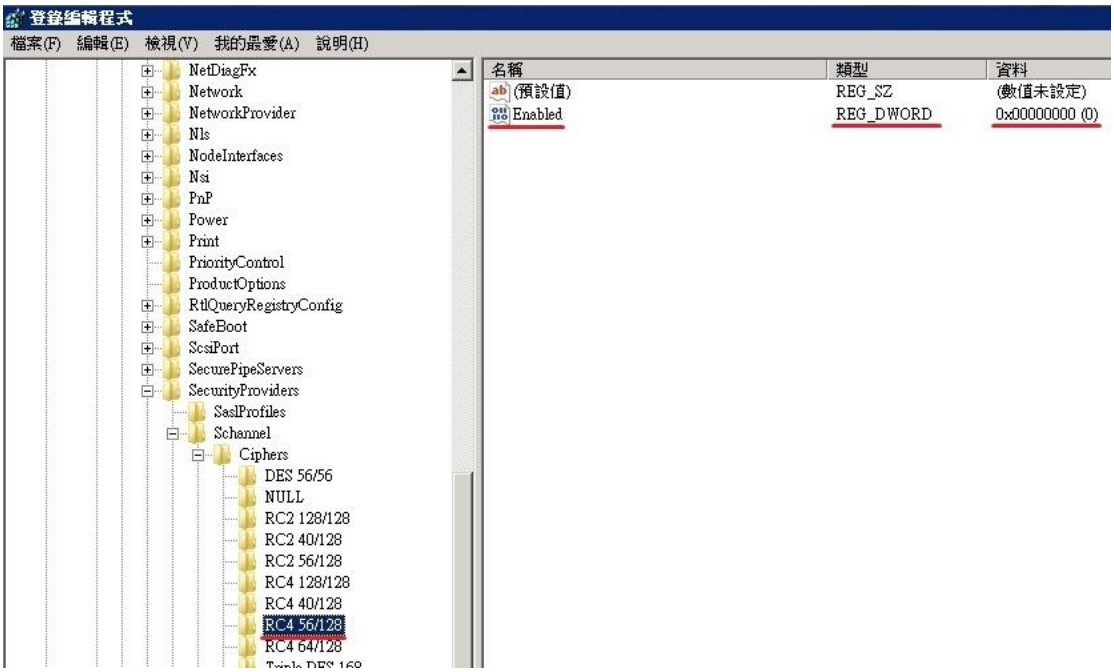

登錄編輯程式
檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 說明(H)
NetDiagFx
Network
NetworkProvider
Nls
NodeInterfaces
Nsi
PnP
Power
Print
PriorityControl
ProductOptions
RtlQueryRegistryConfig
SafeBoot
ScsiPort
SecurePipeServers
SecurityProviders
SaslProfiles
Schannel
Ciphers
DES 56/56
NULL
RC2 128/128
RC2 40/128
RC2 56/128
RC4 128/128
RC4 40/128
RC4 56/128
RC4 64/128
名稱
類型
資料
(預設值)
REG_SZ
(數值未設定)
Enabled
REG_DWORD
0x00000000 (0)

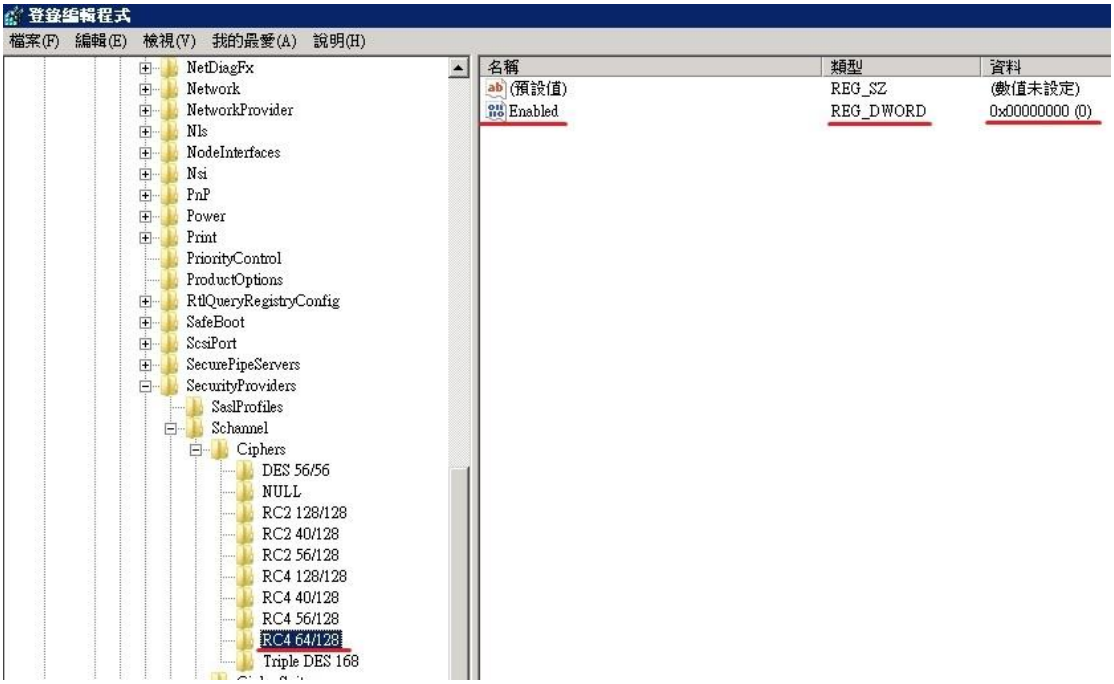

登錄編輯程式
檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 說明(H)
NetDiagFx
Network
NetworkProvider
Nls
NodeInterfaces
Nsi
PnP
Power
Print
PriorityControl
ProductOptions
RtlQueryRegistryConfig
SafeBoot
ScsiPort
SecurePipeServers
SecurityProviders
SaslProfiles
Schannel
Ciphers
DES 56/56
NULL
RC2 128/128
RC2 40/128
RC2 56/128
RC4 128/128
RC4 40/128
名稱
類型
資料
(預設值)
REG_SZ
(數值未設定)
Enabled
REG_DWORD
0x00000000 (0)

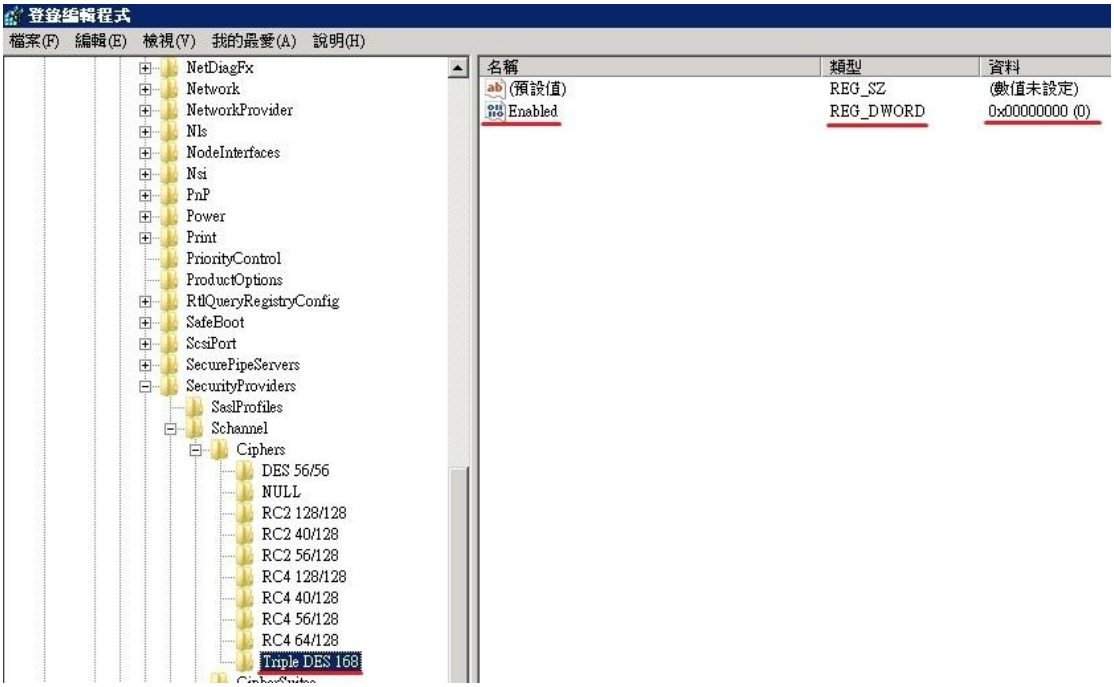

登錄編輯程式
檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 說明(H)
NetDiagFx
Network
NetworkProvider
Nls
NodeInterfaces
Nsi
PnP
Power
Print
PriorityControl
ProductOptions
RtlQueryRegistryConfig
SafeBoot
ScsiPort
SecurePipeServers
SecurityProviders
SaslProfiles
Schannel
Ciphers
DES 56/56
NULL
RC2 128/128
RC2 40/128
RC2 56/128
RC4 128/128
RC4 40/128
RC4 56/128
名稱
類型
資料
(預設值)
REG_SZ
(數值未設定)
Enabled
REG_DWORD
0x00000000 (0)


登錄編輯程式
檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 說明(H)
NetDiagFx
Network
NetworkProvider
Nls
NodeInterfaces
Nsi
PnP
Power
Print
PriorityControl
ProductOptions
RtlQueryRegistryConfig
SafeBoot
ScsiPort
SecurePipeServers
SecurityProviders
SaslProfiles
Schannel
Ciphers
DES 56/56
NULL
RC2 128/128
RC2 40/128
RC2 56/128
RC4 128/128
RC4 40/128
名稱
類型
資料
(預設值)
REG_SZ
(數值未設定)
Enabled
REG_DWORD
0x00000000 (0)

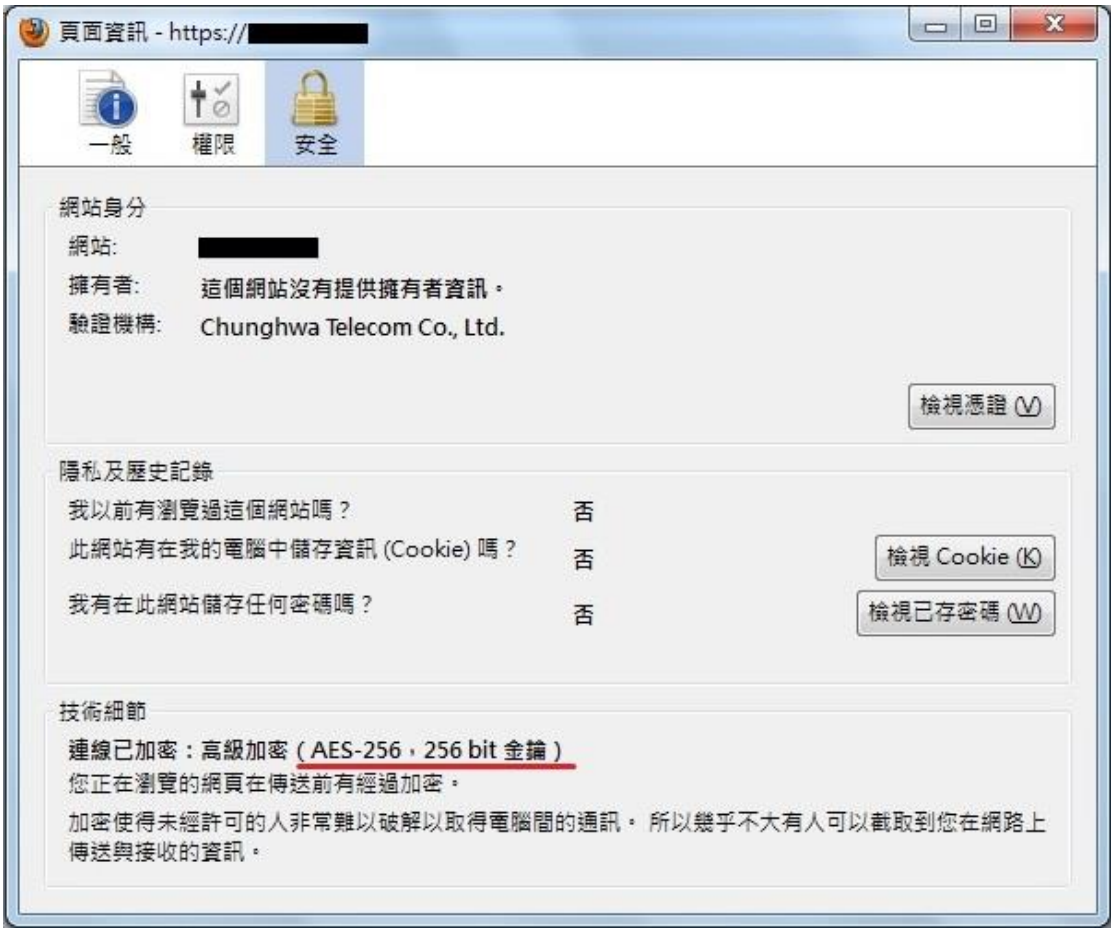

登錄編輯程式
檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 說明(H)
NetDiagFx
Network
NetworkProvider
Nls
NodeInterfaces
Nsi
PnP
Power
Print
PriorityControl
ProductOptions
RtlQueryRegistryConfig
SafeBoot
ScsiPort
SecurePipeServers
SecurityProviders
SaslProfiles
Schannel
Ciphers
DES 56/56
NULL
RC2 128/128
RC2 40/128
RC2 56/128
RC4 128/128
RC4 40/128
RC4 56/128
名稱
類型
資料
(預設值)
REG_SZ
(數值未設定)
Enabled
REG_DWORD
0x00000000 (0)


登錄編輯程式
檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 說明(H)
NetDiagFx
Network
NetworkProvider
Nls
NodeInterfaces
Nsi
PnP
Power
Print
PriorityControl
ProductOptions
RtlQueryRegistryConfig
SafeBoot
ScsiPort
SecurePipeServers
SecurityProviders
SaslProfiles
Schannel
Ciphers
DES 56/56
NULL
RC2 128/128
RC2 40/128
RC2 56/128
RC4 128/128
RC4 40/128
RC4 56/128
RC4 64/128
名稱
類型
資料
(預設值)
REG_SZ
(數值未設定)
Enabled
REG_DWORD
0x00000000 (0)





六、設定完成後，重開機，即可達到 AES 256 位元的加密效果。

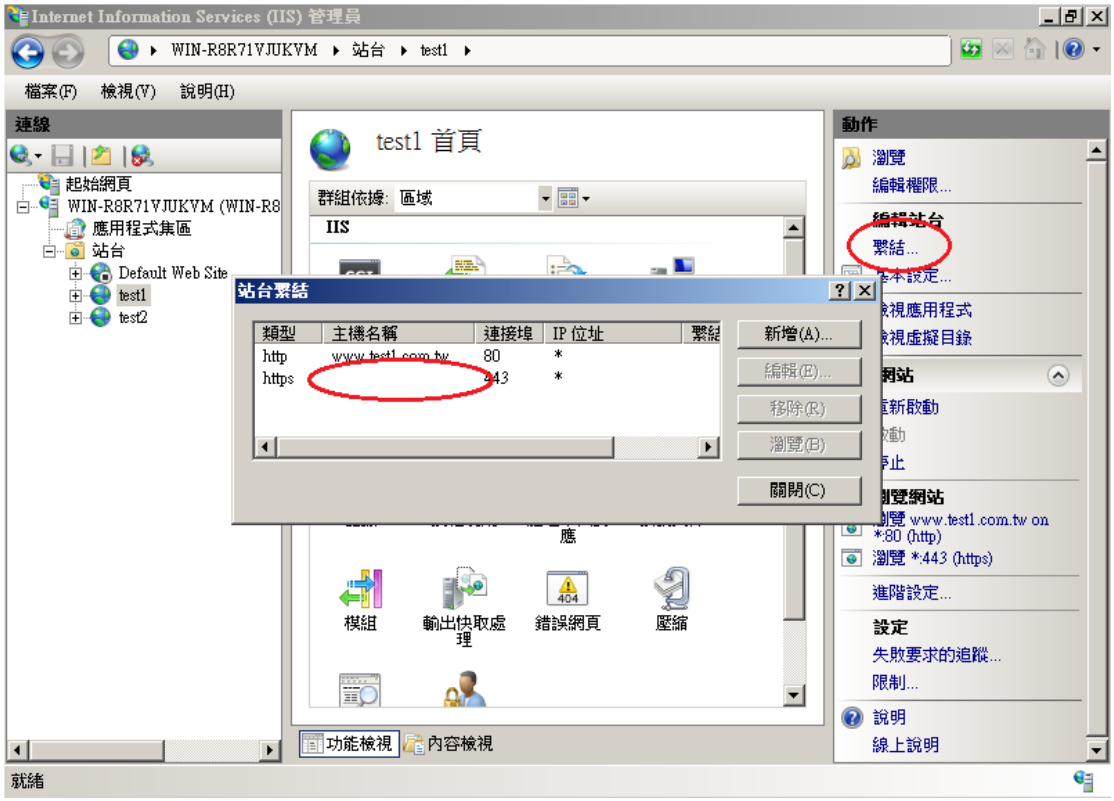

頁面資訊 - https://[redacted]
一般
權限
安全
網站身分
網站: [redacted]
擁有者: 這個網站沒有提供擁有者資訊。
驗證機構: Chunghwa Telecom Co., Ltd.
檢視憑證 (V)
隱私及歷史記錄
我以前有瀏覽過這個網站嗎？ 否
此網站有在我的電腦中儲存資訊 (Cookie) 嗎？ 否
檢視 Cookie (K)
我有在此網站儲存任何密碼嗎？ 否
檢視已存密碼 (W)
技術細節
連線已加密：高級加密（AES-256，256 bit 金鑰）
您正在瀏覽的網頁在傳送前有經過加密。
加密使得未經許可的人非常難以破解以取得電腦間的通訊。 所以幾乎不大有人可以截取到您在網路上傳送與接收的資訊。

附件二：單一 IP，多站台啟用 SSL

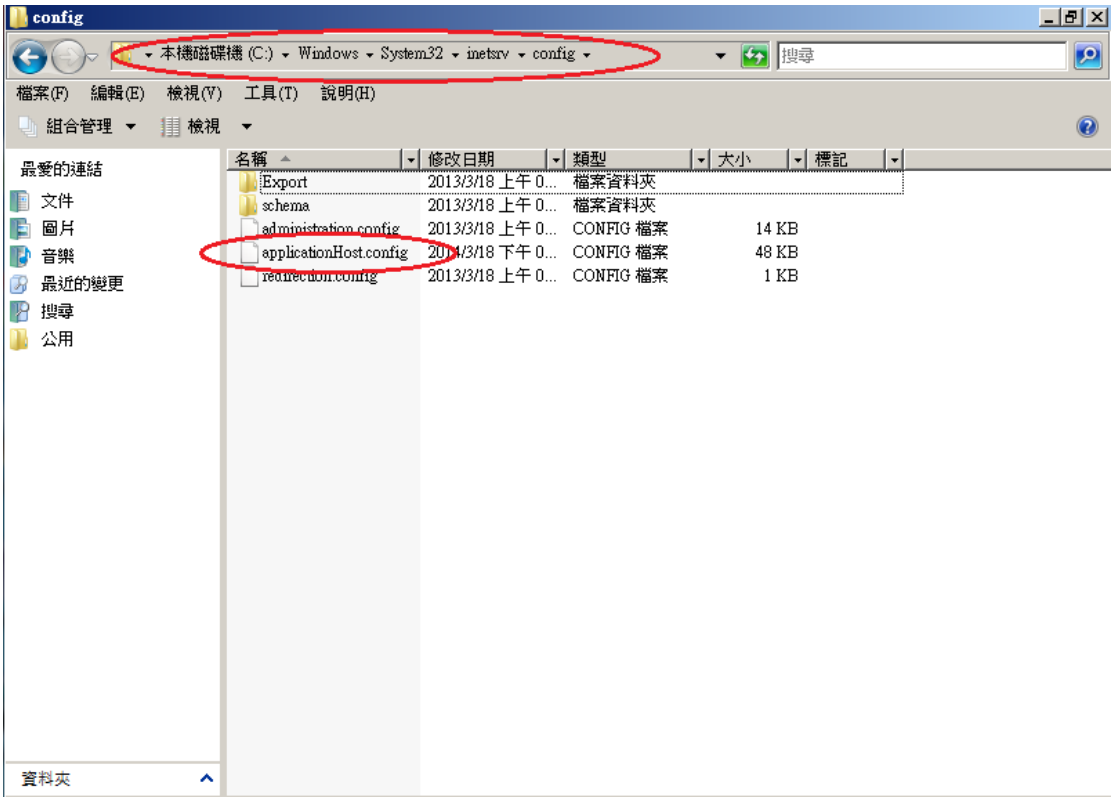
IIS7 在只有一個 IP 的情況下，預設只能有一個網站使用 443 port。依照以下步驟操作，即可在多個網站上啟用 443 port。

一、依照前述的憑證安裝步驟，先在其中一網站上安裝憑證，並以 HTTPS 測試連線是否正常。

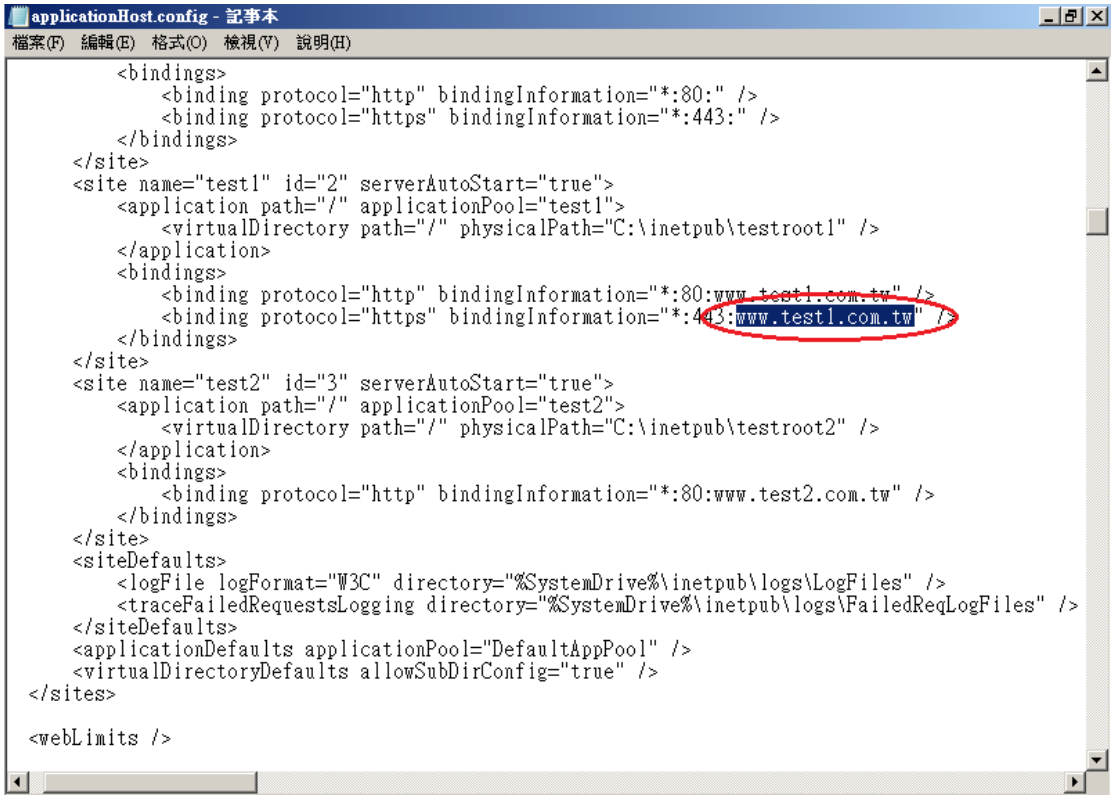
二、再點選 1 次「繫結」，會看到主機名稱下面是空的。



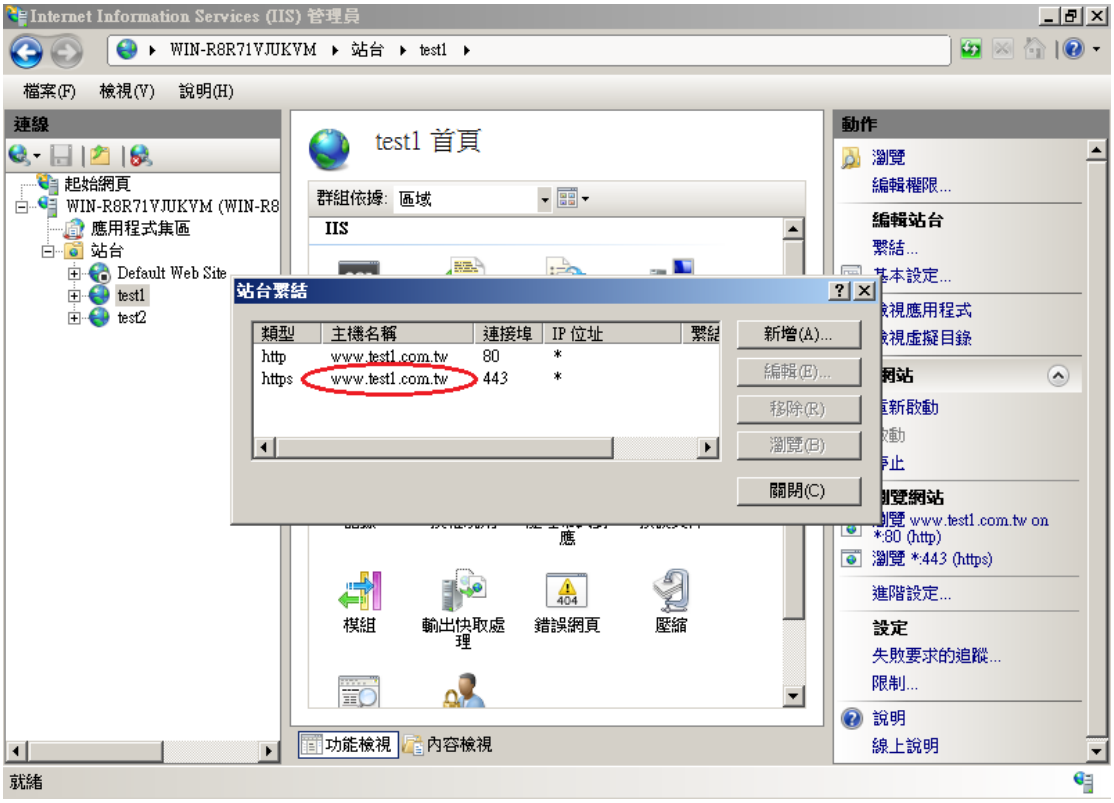
三、到以下目錄：「C:\Windows\System32\inetsrv\config」，以記事本開啟「applicatiuonHost.config」



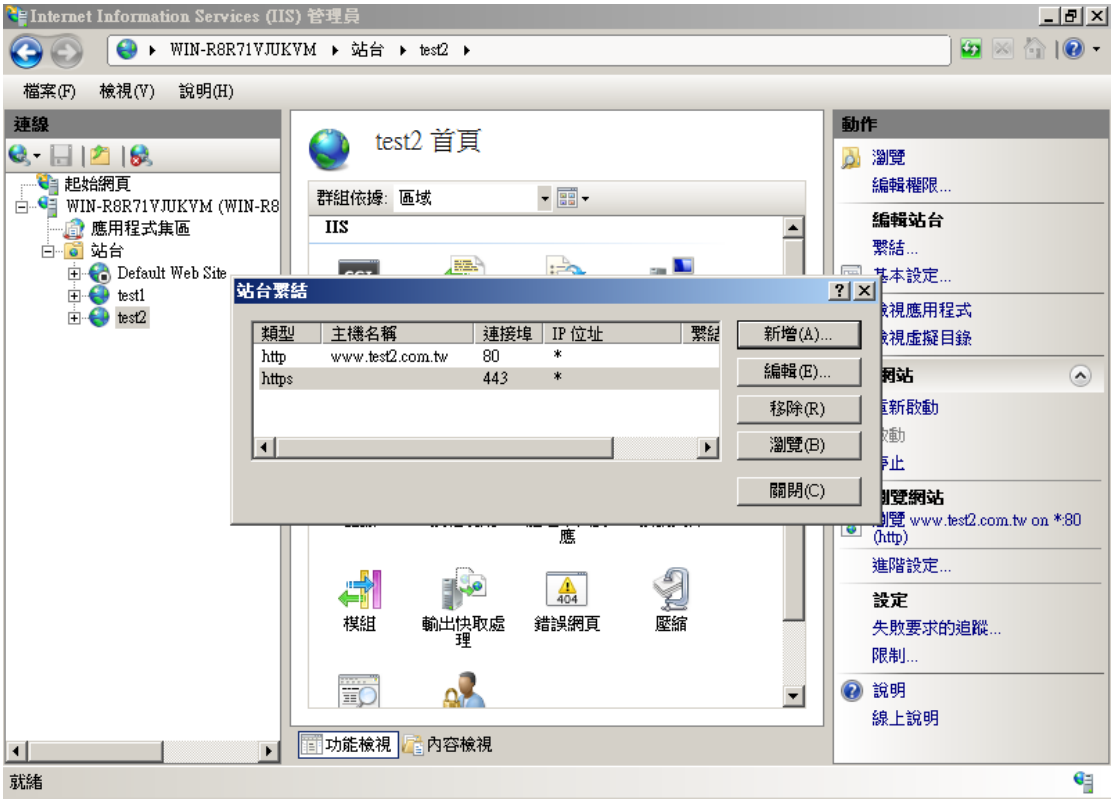
四、找到剛剛有新增 443 port 的網站後，將 domain name 加入 443：之後，存檔並關閉，如圖。

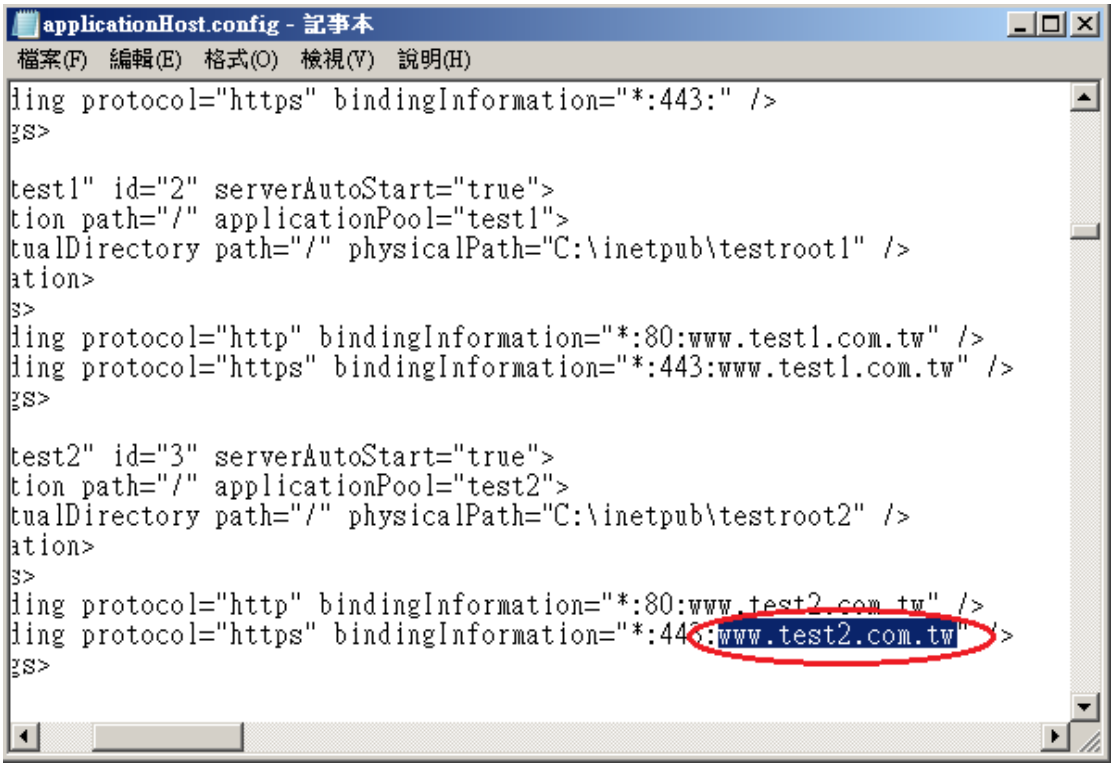


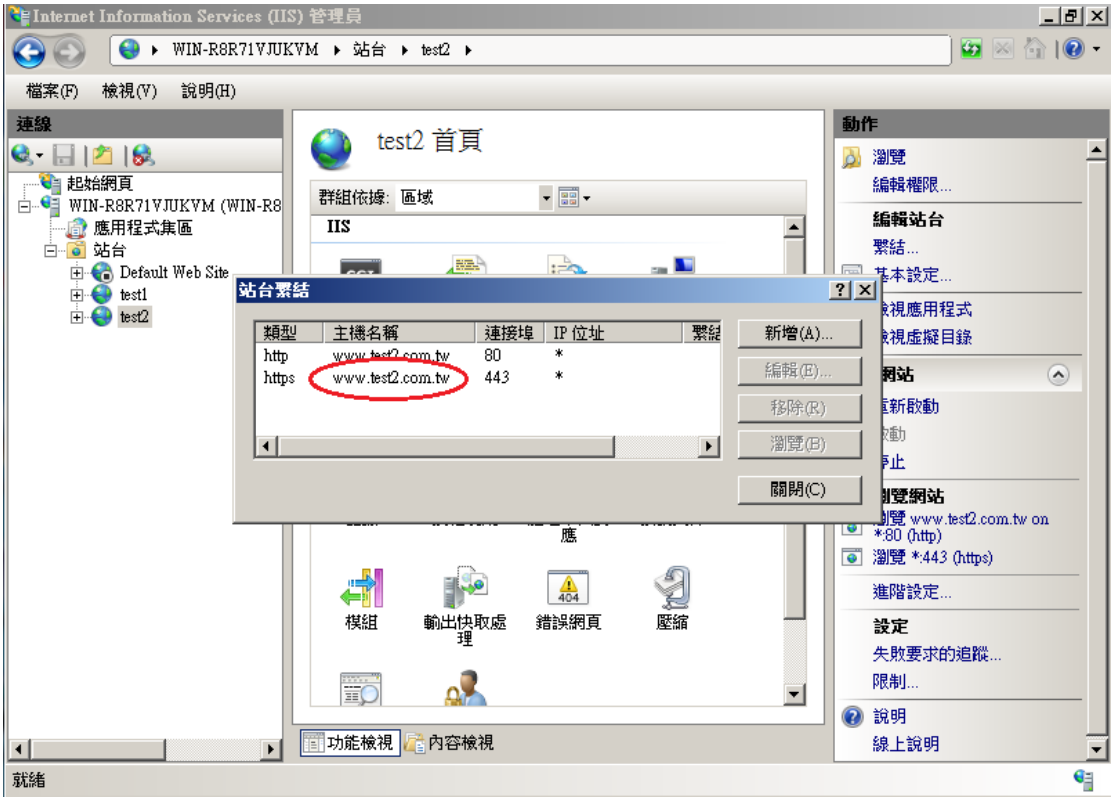
五、回 IIS 管理員，重新點選「繫結」，會看到主機名稱下出現之前輸入的 domain name，這樣即表示修改成功。



六、接著，可以先將第 2 個網站新增 443 port 以及掛上憑證，同樣去修改「applicatiuonHost.config」







七、其他需要掛上憑證的網站依照上述步驟操作。完成後，請以HTTPS連線測試，是否所有網站皆正常。